

Ethernet PrintServer mit integriertem Multiprotokoll und Wireless Ethernet PrintServer

NETZWERKHANDBUCH



Dieses Netzwerkhandbuch enthält nützliche Informationen zu den LAN- und WLAN-Einstellungen und Sicherheitseinstellungen, die von Ihrem Brother-Gerät verwendet werden. Sie finden hier auch Informationen zu den unterstützten Protokollen und ausführliche Hinweise zur Problemlösung.

Grundlegende Informationen zu Netzwerkfunktionen und zu den erweiterten Netzwerkfunktionen Ihres Brother-Gerätes finden Sie im Handbuch *Netzwerkbegriffe*.

Das neueste Handbuch können Sie vom Brother Solutions Center unter http://solutions.brother.com/ herunterladen. Sie können im Brother Solutions Center auch die neuesten Treiber und Dienstprogramme für Ihr Gerät herunterladen, Antworten auf häufig gestellte Fragen (FAQs) und Tipps zur Problemlösung finden oder sich über besondere Lösungen rund um das Drucken informieren.

Version 0

GER

Definition der Hinweise

In diesem Handbuch werden die folgenden Symbole verwendet:

WICHTIG	WICHTIG weist auf eine potentiell gefährliche Situation hin, die zu Sachschäden oder zu Funktionsausfall des Gerätes führen kann.
Hinweis	Hinweise informieren Sie, wie auf eine bestimmte Situation reagiert werden sollte, oder geben Ihnen hilfreiche Tipps zur beschriebenen Funktion.

WICHTIGER HINWEIS

- Dieses Produkt ist nur zur Verwendung in dem Land zugelassen, in dem es gekauft wurde. Verwenden Sie dieses Produkt daher nur in dem Land, in dem Sie es gekauft haben, da es in anderen Ländern eventuell gegen die Telekommunikationsbestimmungen und Anschlussvorschriften verstößt.
- Windows® XP steht in diesem Dokument für Windows® XP Professional, Windows® XP Professional x64 Edition und Windows® XP Home Edition.
- Windows Server® 2003 steht in diesem Dokument für Windows Server® 2003 und Windows Server® 2003 x64 Edition.
- Windows Server® 2008 steht in diesem Dokument für Windows Server® 2008 und Windows Server® 2008 R2.
- Windows Vista® steht in diesem Handbuch für alle Ausgaben von Windows Vista®.
- Windows® 7 steht in diesem Handbuch für alle Ausgaben von Windows® 7.
- Bitte besuchen Sie das Brother Solutions Center unter http://solutions.brother.com/ und klicken Sie auf der Seite für Ihr Modell auf , um die anderen Handbücher herunterzuladen.
- Nicht alle Modelle sind in allen Ländern verfügbar.

Inhaltsverzeichnis

7 Sicherheitsfunktionen 51

8 Problemlösung 73

A Anhang A 81

B Stichwortverzeichnis 82

1 Einführung

Netzwerkfunktionen

Ihr Brother-Gerät kann durch den internen Netzwerk-PrintServer gemeinsam über ein verkabeltes 10/100 MB oder ein drahtloses IEEE 802.11b/g Ethernet-Netzwerk genutzt werden. Der PrintServer bietet vielfältige Funktionen und unterstützt verschiedene Verbindungsverfahren, je nachdem mit welchem Betriebssystem Sie in Ihrem TCP/IP-fähigen Netzwerk arbeiten. Die folgende Tabelle zeigt, welche Netzwerkfunktionen und -verbindungen von den einzelnen Betriebssystemen unterstützt werden.



Hinweis

Obwohl das Brother-Gerät sowohl in einem Wireless-Netzwerk als auch in einem verkabelten Netzwerk verwendet werden kann, können nicht beide Verbindungsmethoden gleichzeitig genutzt werden.

Betriebssysteme	Windows® 2000/XP Windows Vista® Windows® 7	Windows Server® 2003/2008	Mac OS X 10.4.11 - 10.6.x
Drucken	✔	✔	✔
BRAdmin Light Siehe Seite 3.	✔	✔	✔
BRAdmin Professional 3 [1] Siehe Seite 6.	✔	✔	
Web BRAdmin [1] Siehe Seite 7.	✔	✔	
Web Based Management (Webbrowser) Siehe Seite 40.	✔	✔	✔
Status Monitor Siehe *Benutzerhandbuch*.	✔	✔	✔
Treiberinstallations-Assistent	✔	✔	
Vertical Pairing (WLAN-Einrichtungsassistent) Siehe *Netzwerkbegriffe*.	✔ [2]		

[1] BRAdmin Professional 3 und Web BRAdmin können von http://solutions.brother.com/ heruntergeladen werden.

[2] Nur Windows® 7

Sonstige Netzwerkfunktionen

Sicherheit

Ihr Brother-Gerät verwendet moderne Protokolle zur Netzwerksicherheit und Datenverschlüsselung. (Siehe *Sicherheitsfunktionen* auf Seite 51.)

Benutzersperre 2.0

Die Benutzersperre 2.0 erhöht die Sicherheit durch die Möglichkeit, die Verwendung von Funktionen zu sperren. (Siehe *Benutzersperre 2.0* auf Seite 42.)

Druckprotokoll im Netzwerk speichern

Die Funktion “Druckprotokoll im Netzwerk speichern” ermöglicht das Speichern der Druckprotokoll-Datei Ihres Brother-Gerätes auf einem Netzwerkserver unter Verwendung von CIFS. (Siehe *Druckprotokoll im Netzwerk speichern* auf Seite 46.)

2 Netzwerkeinstellungen des Gerätes ändern

So können die Netzwerkeinstellungen des Gerätes geändert werden (IP-Adresse, Subnetzmaske und Gateway)

Funktionstastenfeld verwenden

Sie können das Gerät zur Verwendung im Netzwerk über das Funktionstasten-Menü `Netzwerk` konfigurieren. (Siehe *Einstellungen über das Funktionstastenfeld* auf Seite 31.)

Dienstprogramm BRAdmin Light verwenden

Das Dienstprogramm BRAdmin Light wurde für die Ersteinrichtung von netzwerkfähigen Brother-Geräten entwickelt. In einer TCP/IP-Umgebung können Sie damit auch nach Brother-Geräten suchen, deren Status anzeigen und grundlegende Netzwerkeinstellungen, wie die IP-Adresse, vornehmen.

BRAdmin Light installieren

- Windows®

  1. Vergewissern Sie sich, dass das Gerät eingeschaltet ist.
  2. Schalten Sie den Computer ein. Schließen Sie alle Anwendungen, bevor Sie mit der Konfiguration beginnen.
  3. Legen Sie die mitgelieferte CD-ROM in das CD-ROM-Laufwerk ein. Der Startbildschirm wird automatisch angezeigt. Wenn der Bildschirm zur Auswahl des Modells erscheint, wählen Sie Ihr Modell. Wenn der Bildschirm zur Auswahl der Sprache erscheint, wählen Sie Ihre Sprache.
  4. Das Hauptmenü der CD-ROM wird angezeigt. Klicken Sie auf **Andere Treiber/Programme installieren**.
  5. Klicken Sie auf **BRAdmin Light** und folgen Sie den Anweisungen auf dem Bildschirm.

- Macintosh

  Die Software BRAdmin Light wird automatisch bei der Installation des Druckertreibers mitinstalliert. Falls Sie den Druckertreiber bereits installiert haben, müssen Sie BRAdmin Light nicht erneut installieren.

IP-Adresse, Subnetzmaske und Gateway mit BRAdmin Light einstellen

Hinweis

- Sie können die neueste Version von Brother BRAdmin Light von http://solutions.brother.com/ herunterladen.
- Wenn Sie ein erweitertes Geräteverwaltungsprogramm benötigen, sollten Sie die neuste Version von BRAdmin Professional 3 verwenden, die von http://solutions.brother.com/ heruntergeladen werden kann. Dieses Dienstprogramm ist nur für Windows® verfügbar.
- Falls Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, aktivieren Sie die Anwendung wieder.
- Knotenname: Der Knotenname wird im aktuellen BRAdmin-Light-Fenster angezeigt. Der Standardknotenname des PrintServers Ihres Gerätes ist “BRNxxxxxxxxxxxx” für ein verkabeltes Netzwerk bzw. “BRWxxxxxxxxxxxx” für ein Wireless-Netzwerk. (“xxxxxxxxxxxx” steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)
- Das Standardkennwort für den Brother-PrintServer ist „access“.

1. Starten Sie BRAdmin Light.

   - Windows®

     Klicken Sie auf **Start** / **Alle Programme** [1] / **Brother** / **BRAdmin Light** / **BRAdmin Light**.

     [1] **Programme** für Nutzer von Windows® 2000

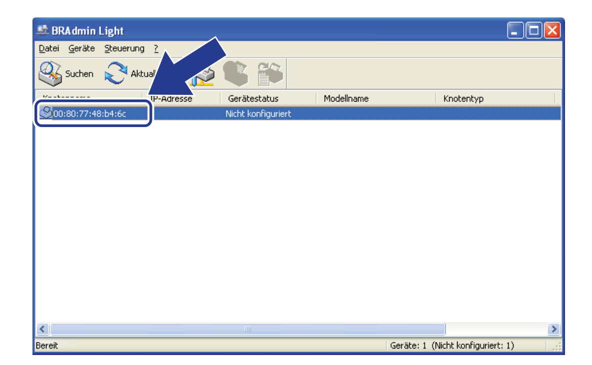
   - Macintosh

     Doppelklicken Sie auf **Macintosh HD** (Startvolume) / **Library** / **Printers** / **Brother** / **Utilities** / **BRAdmin Light.jar**.

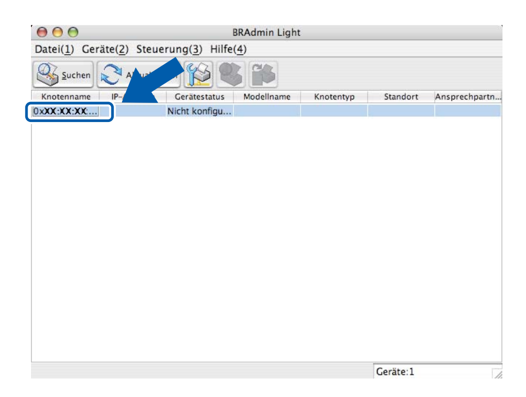
2. BRAdmin Light sucht nun automatisch nach neuen Geräten.

3 Doppelklicken Sie auf das nicht konfigurierte Gerät.

Windows®



Macintosh

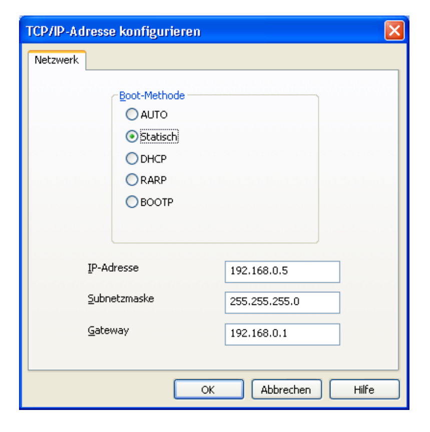


Hinweis

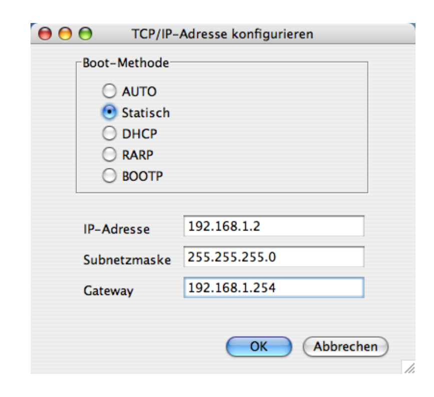
- Sind für den PrintServer die werkseitigen Standardeinstellungen eingestellt (wenn Sie keinen DHCP/BOOTP/RARP-Server verwenden) wird das Gerät in BRAdmin Light als **Nicht konfiguriert** angezeigt.
- Den Knotennamen und die MAC-Adresse (Ethernet-Adresse) können Sie dem Ausdruck der Netzwerk-Konfigurationsliste Ihres PrintServers entnehmen. (Unter *Netzwerk-Konfigurationsliste drucken* auf Seite 35 finden Sie nähere Informationen zum Drucken der Netzwerk-Konfigurationsliste.) Sie können die MAC-Adresse auch über das Funktionstastenfeld ermitteln. (Siehe *Kapitel 5: Einstellungen über das Funktionstastenfeld*.)

4 Wählen Sie **Statisch** im Feld **Boot-Methode**. Geben Sie **IP-Adresse**, **Subnetzmaske** und **Gateway** (soweit erforderlich) des PrintServers ein.

Windows®



Macintosh



5 Klicken Sie auf **OK**.

6 Ist die IP-Adresse korrekt, wird der Brother-PrintServer in der Geräteliste angezeigt.

Andere Verwaltungsprogramme

Für Ihr Brother-Gerät stehen neben dem Dienstprogramm BRAdmin Light noch die folgenden Verwaltungsprogramme zur Verfügung. Mit diesen Programmen können Sie Ihre Netzwerkeinstellungen ändern.

Web Based Management (Webbrowser)

Sie können die Einstellungen des PrintServers über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) ändern. (Siehe *Geräteeinstellungen mit dem Web Based Management (Webbrowser) konfigurieren* auf Seite 40.)

BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 ist ein Dienstprogramm für die erweiterte Verwaltung von netzwerkfähigen Brother-Geräten. Sie können mit diesem Dienstprogramm nach Brother-Geräten im Netzwerk suchen und den Gerätestatus in einem leicht lesbaren Explorer-artigen Fenster ansehen, das die Farbe ändert, um den Status der einzelnen Geräte anzuzeigen. Daneben können Sie mit einem Windows®-Computer in Ihrem LAN Netzwerk- und Geräteeinstellungen ändern und die Firmware aktualisieren. BRAdmin Professional 3 kann auch die Aktivitäten von Brother-Geräte im Netzwerk protokollieren und die Protokolldaten in das HTML-, CSV-, TXT- oder SQL-Format exportieren.

Nutzer, die lokal angeschlossene Geräte überwachen möchten, sollten die Print Auditor Client-Software auf ihrem Client-PC installieren. Dieses Dienstprogramm ermöglicht es, auch solche Geräte mit BRAdmin Professional 3 zu überwachen, die über die USB- oder die parallele Schnittstelle an den Client-PC angeschlossen sind.

Besuchen Sie uns unter http://solutions.brother.com/, um weitere Informationen zu erhalten und die Software herunterzuladen.

Hinweis

- Sie sollten die neueste Version von BRAdmin Professional 3 verwenden, die Sie von http://solutions.brother.com/ herunterladen können. Dieses Dienstprogramm ist nur für Windows® verfügbar.
- Wenn Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, konfigurieren Sie die Software-Einstellungen entsprechend den Anweisungen erneut.
- Knotenname: Der Knotenname der einzelnen Brother-Geräte im Netzwerk wird in BRAdmin Professional 3 angezeigt. Der Standardknotenname ist „BRNxxxxxxxxxxxx“ für ein verkabeltes Netzwerk und „BRWxxxxxxxxxxxx“ für ein Wireless-Netzwerk. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

Web BRAdmin (Windows®)

Web BRAdmin ist ein Dienstprogramm zur Verwaltung von netzwerkfähigen Brother-Geräten Sie können mit diesem Dienstprogramm nach Brother-Geräten im Netzwerk suchen, den Status anzeigen und Netzwerkeinstellungen konfigurieren.

Anders als BRAdmin Professional 3, das nur für Windows®-Systeme geeignet ist, kann die serverbasierte Software Web BRAdmin von jedem Client-Computer mit einem JRE-fähigen Browser (Java Runtime Environment) verwendet werden. Nach der Installation der Server-Software Web BRAdmin auf einem Computer mit IIS [1] können Administratoren mit einem Webbrowser eine Verbindung zum Web-BRAdmin-Server herstellen, der dann seinerseits mit dem Zielgerät kommuniziert.

Besuchen Sie uns unter http://solutions.brother.com/, um weitere Informationen zu erhalten und die Software herunterzuladen.

[1] Internet Information Server 4.0 oder Internet Information Services 5.0/5.1/6.0/7.0

BRPrint Auditor (Windows®)

Die BRPrint Auditor-Software ermöglicht es, die Überwachungsfunktionen der Brother Netzwerkverwaltungsprogramme auch für lokal angeschlossene Geräte zu verwenden. Mit Hilfe dieses Dienstprogramms kann ein Client-Computer Nutzungs- und Statusinformationen von einem Brother-Gerät abrufen, das über eine Parallel- oder USB-Schnittstelle angeschlossen ist. Der BRPrint Auditor kann diese Informationen dann zu einem anderen Computer im Netzwerk weiterleiten, auf dem BRAdmin Professional 3 oder Web BRAdmin 1.45 oder eine höhere Version ausgeführt wird. Dadurch kann der Administrator verschiedene Informationen wie den Seitenzähler, den Toner- und Trommelstatus und die Firmware-Version abrufen und prüfen. Dieses Dienstprogramm kann die Nutzungs- und Statusinformationen aber nicht nur an die Brother-Netzwerkverwaltungsanwendungen weiterleiten, sondern auch per E-Mail im CSV- oder XML-Dateiformat direkt an eine voreingestellte E-Mail-Adresse senden (SMTP-Mailunterstützung ist erforderlich). Das BRPrint Auditor-Dienstprogramm unterstützt darüber hinaus auch die E-Mail-Benachrichtigungsfunktion zum Anzeigen von Warnmeldungen und Fehlerbedingungen.

3 Gerät für ein Wireless-Netzwerk konfigurieren (für HL-4570CDW(T))

Übersicht

Zur Einrichtung Ihres Gerätes im Wireless-Netzwerk empfehlen wir, dass Sie die Schritte in der *Installationsanleitung* zur Verwendung des WPS- bzw. AOSS™-Funktionsmenüs auszuführen. Mit dieser Methode können Sie Ihr Gerät einfach im Wireless-Netzwerk anschließen.

In diesem Kapitel werden weitere Verfahren zur Konfiguration der Wireless-Netzwerkeinstellungen beschrieben. Informationen zu TCP/IP-Einstellungen finden Sie unter *So können die Netzwerkeinstellungen des Gerätes geändert werden (IP-Adresse, Subnetzmaske und Gateway)* auf Seite 3.

Hinweis

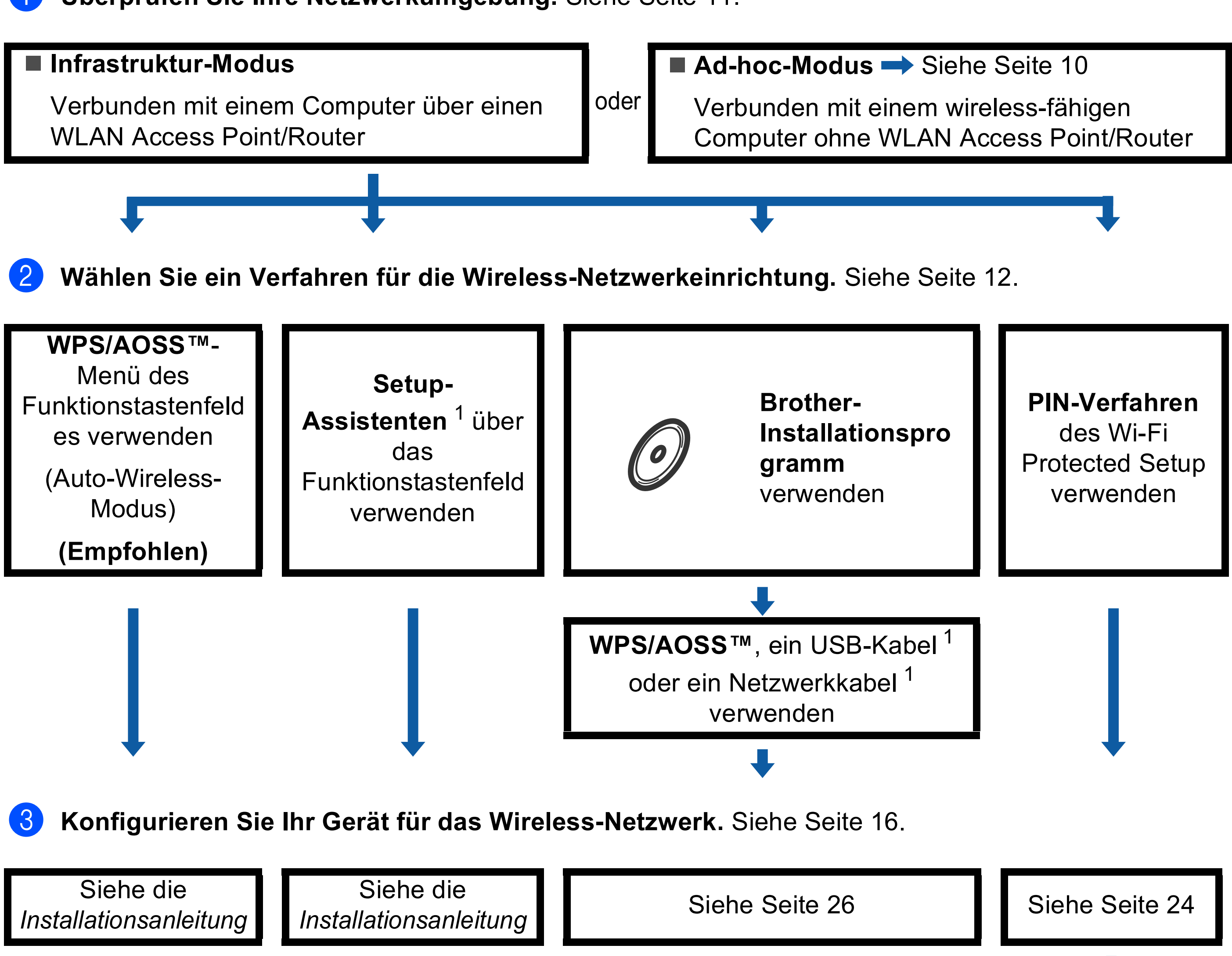
- Zur Erzielung optimaler Ergebnisse beim alltäglichen Drucken von Dokumenten sollten Sie das Brother-Gerät möglichst nah am WLAN Access Point/Router des Netzwerkes aufstellen und darauf achten, dass keine Hindernisse den Funkkontakt beeinträchtigen. Große Gegenstände und Wände zwischen den beiden Geräten sowie Funkstörungen durch andere elektronische Einrichtungen können die Geschwindigkeit der Datenübertragung beeinträchtigen.

  Daher ist eine drahtlose Verbindung möglicherweise nicht die beste Verbindungsmethode zur Übertragung aller Dokumentenarten und Anwendungen. Wenn Sie große Dateien wie mehrseitige Dokumente mit Text und großen Grafiken drucken, ist es überlegenswert, ein verkabeltes Ethernet-Netzwerk für einen schnelleren Datentransfer oder eine USB-Verbindung zum Erreichen der höchsten Übertragungsgeschwindigkeit zu wählen.
- Obwohl das Brother-Gerät sowohl in einem Wireless-Netzwerk als auch in einem verkabelten Netzwerk verwendet werden kann, können nicht beide Verbindungsmethoden gleichzeitig genutzt werden.
- Bevor Sie die Wireless-Einstellungen konfigurieren, müssen Sie Ihren Netzwerknamen (SSID, ESSID) und Ihren Netzwerkschlüssel kennen. Wenn Sie ein Wireless-Firmennetzwerk verwenden, müssen Sie auch die Benutzer-ID und das Kennwort wissen.

Schritte zur Wireless-Netzwerkkonfiguration

Für den Infrastruktur-Modus

1 **Überprüfen Sie Ihre Netzwerkumgebung.** Siehe Seite 11.



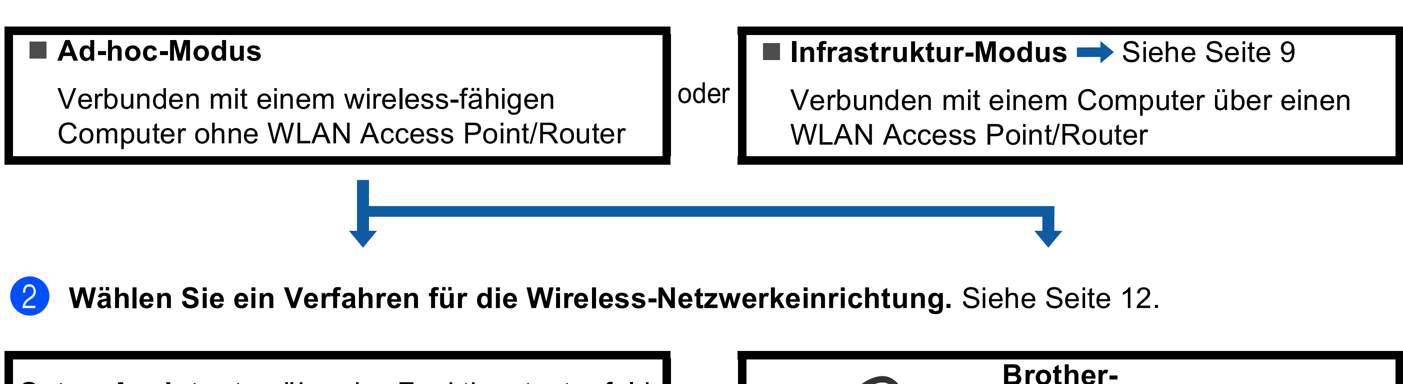
Druckertreiber installieren (siehe die *Installationsanleitung*)

[1] Mit IEEE 802.1x-Unterstützung

OK! **Die Wireless-Konfiguration und die Installation des Druckertreibers sind abgeschlossen.**

Für den Ad-hoc-Modus

1 **Überprüfen Sie Ihre Netzwerkumgebung.** Siehe Seite 11.

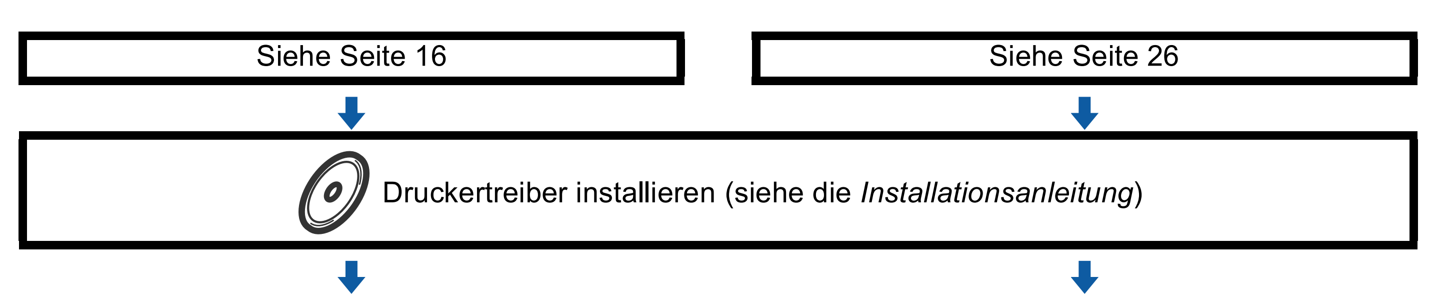


2 **Wählen Sie ein Verfahren für die Wireless-Netzwerkeinrichtung.** Siehe Seite 12.

Setup-Assistenten über das Funktionstastenfeld verwenden **(Empfohlen)**



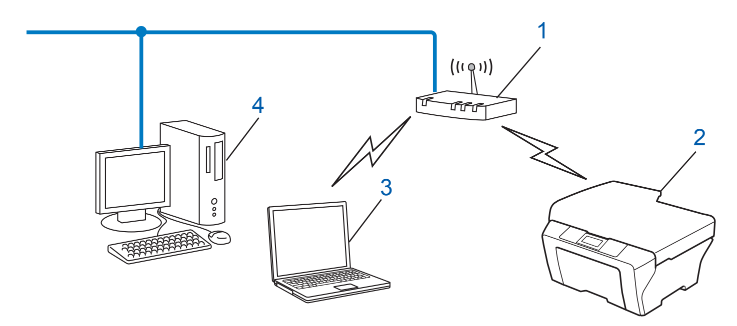
3 **Konfigurieren Sie Ihr Gerät für das Wireless-Netzwerk.** Siehe Seite 16.



OK! **Die Wireless-Konfiguration und die Installation des Druckertreibers sind abgeschlossen.**

Überprüfen Sie Ihre Netzwerkumgebung

Verbunden mit einem Computer über einen WLAN Access Point/Router im Netzwerk (Infrastruktur-Modus)



1 WLAN Access Point/Router [1]

[1] Wenn Ihr Computer Intel® MWT (My WiFi Technology) unterstützt, können Sie Ihren Computer wie einen Wi-Fi Protected Setup unterstützenden Access Point verwenden.

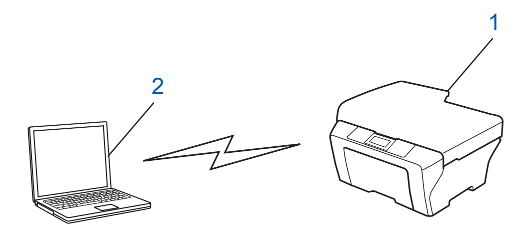
2 Wireless-Netzwerkgerät (Ihr Gerät)

3 Mit dem WLAN Access Point/Router verbundener wireless-fähiger Computer

4 Verkabelter Computer (nicht wireless-fähig) über ein Ethernetkabel mit dem WLAN Access Point verbunden

Verbunden mit einem wireless-fähigen Computer ohne einen WLAN Access Point im Netzwerk (Ad-hoc-Modus)

Bei diesem Netzwerktyp gibt es keinen zentralen Zugriffspunkt (WLAN Access Point). Alle Wireless-Geräte kommunizieren direkt miteinander. Wenn das Brother Wireless-Gerät (Ihr Gerät) Teil dieses Netzwerkes ist, erhält es alle Druckaufträge direkt von dem Computer, der die Druckdaten sendet.



1 Wireless-Netzwerkgerät (Ihr Gerät)

2 Wireless-fähiger Computer



Hinweis

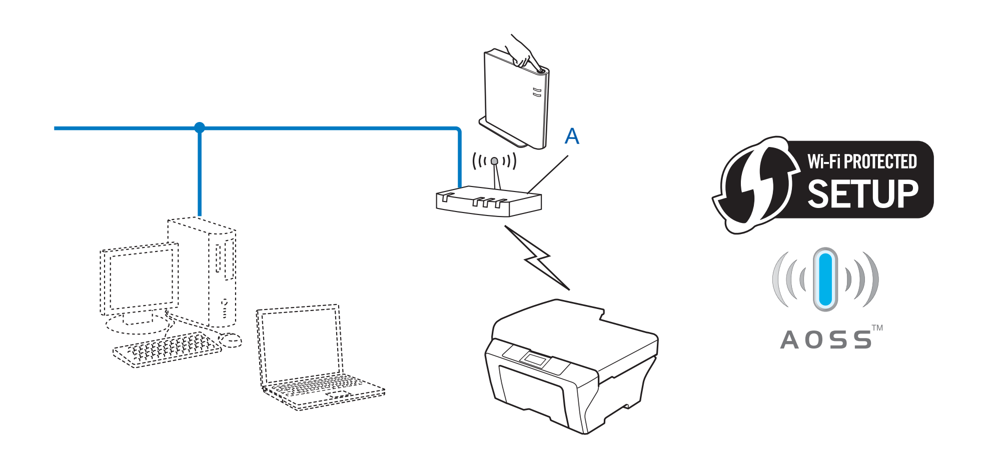
Wir garantieren nicht für eine Wireless-Netzwerkverbindung mit Windows Server®-Produkten im Ad-hoc-Modus.

Wählen Sie ein Verfahren für die Wireless-Netzwerkeinrichtung

Zur Konfiguration Ihres Wireless-Netzwerkgerätes stehen vier Verfahren zur Verfügung. Verwenden Sie WPS/AOSS™ über das Menü des Funktionstastenfeldes (empfohlen), den Setup-Assistenten über das Funktionstastenfeld, das Brother-Installationsprogramm auf der CD-ROM oder das PIN-Verfahren von Wi-Fi Protected Setup. Je nach Netzwerkumgebung verläuft die Einrichtung unterschiedlich.

Wireless-Netzwerkgerät über das WPS/AOSS™-Menü des Funktionstastenfeldes konfigurieren (Auto-Wireless-Modus) (nur Infrastruktur-Modus) (empfohlen)

Wir empfehlen die Verwendung von WPS oder AOSS™ über das Menü des Funktionstastenfeldes zur Konfiguration der Wireless-Netzwerkeinstellungen, wenn Ihr WLAN Access Point/Router (A) entweder das Wi-Fi Protected Setup (PBC [1]) oder AOSS™ unterstützt.



1 Push Button Configuration (Konfiguration per Tastendruck)

Wireless-Netzwerkgerät mit dem Setup-Assistenten über das Funktionstastenfeld konfigurieren

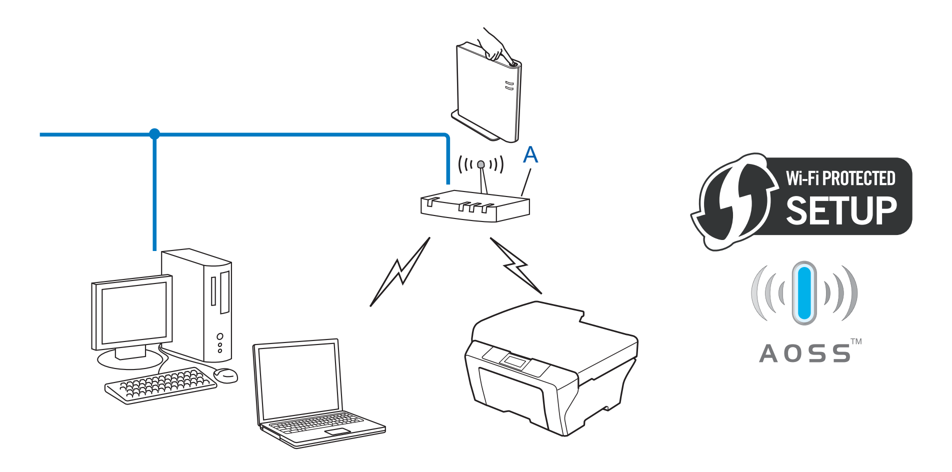
Sie können zur Konfiguration der Wireless-Netzwerkeinstellungen das Funktionstastenfeld des Gerätes verwenden. Mit Hilfe der Funktion `Setup-Assist.` im Menü des Gerätes können Sie Ihr Brother-Gerät einfach mit Ihrem Wireless-Netzwerk verbinden. **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**

Wireless-Netzwerkgerät mit dem Brother-Installationsprogramm auf der CD-ROM konfigurieren

Sie können auch das Brother-Installationsprogramm auf der CD-ROM verwenden, die mit Ihrem Gerät geliefert wurde. Sie werden dann Schritt für Schritt durch die Installation geführt, bis Ihr Brother Wireless-Netzwerkgerät verwendet werden kann. **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**

Konfiguration mit dem Auto-Wireless-Modus

Wenn Ihr WLAN Access Point/Router (A) Wi-Fi Protected Setup (PBC [1]) oder AOSS™ unterstützt, können Sie das Gerät einfach mit dem Brother-Installationsprogramm konfigurieren, ohne die Einstellungen Ihres Wireless-Netzwerkes zu kennen.

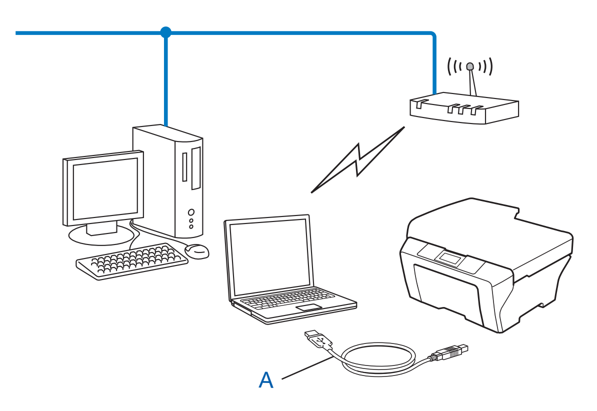


[1] Push Button Configuration (Konfiguration per Tastendruck)

Vorübergehend ein USB- oder Netzwerkkabel zur Konfiguration verwenden

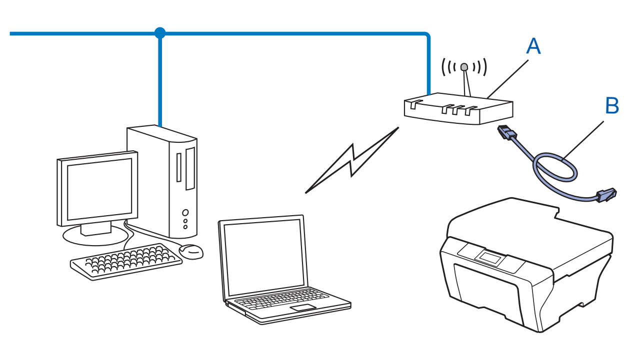
Wenn Sie Ihr Brother-Gerät mit dieser Methode konfigurieren, können Sie vorübergehend ein USB-Kabel oder ein Netzwerkkabel verwenden.

- Sie können das Gerät einfach von einem Computer im Netzwerk aus über ein USB-Kabel konfigurieren (A) [1].



[1] Sie können die Wireless-Einstellungen des Gerätes konfigurieren, indem Sie das Gerät vorübergehend mit einem USB-Kabel an einen verkabelten oder Wireless-Computer anschließen.

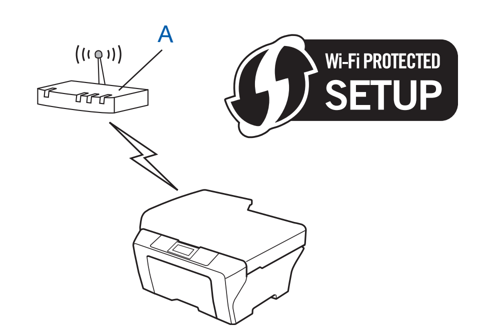
- Wenn neben dem Wireless Access Point (A) Ihres Gerätes auch ein Ethernet-Hub bzw. -Router im selben Netzwerk vorhanden ist, können Sie den Hub bzw. Router vorübergehend über ein Netzwerkkabel (B) an Ihr Gerät anschließen. Sie können dann das Gerät einfach von einem Computer im Netzwerk aus konfigurieren.



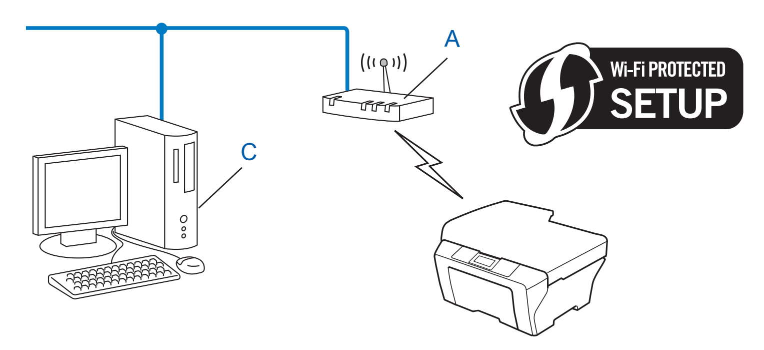
Wireless-Netzwerkgerät mit dem PIN-Verfahren des Wi-Fi Protected Setup konfigurieren (nur Infrastruktur-Modus)

Wenn Ihr WLAN Access Point/Router (A) Wi-Fi Protected Setup unterstützt, können Sie zur Einrichtung auch das PIN-Verfahren des Wi-Fi Protected Setup verwenden.

- Verbindung, wenn der WLAN Access Point/Router (A) auch als Registrar [1] verwendet wird.



- Verbindung, wenn ein anderes Gerät (C) wie z. B. ein Computer als Registrar [1] verwendet wird.



[1] Ein Registrar ist ein Gerät zur Verwaltung des WLANs.

Gerät für ein Wireless-Netzwerk konfigurieren (für Infrastruktur- und Ad-hoc-Modus)

WICHTIG

- Wenn Sie Ihr Brother-Gerät in Ihrem Netzwerk anschließen möchten, sollten Sie sich vor der Installation an Ihren Systemadministrator wenden. **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**
- Falls Sie die Wireless-Einstellungen des Gerätes zuvor schon einmal konfiguriert haben, müssen Sie erst die Netzwerkeinstellungen (LAN) zurücksetzen, bevor Sie die Wireless-Einstellungen erneut konfigurieren können. Drücken Sie **+** oder **-**, um `Netzwerk`, `Netzwerk-Reset`, `Reset` zu wählen, und wählen Sie dann `Ja`, um die Änderung zu bestätigen. Das Gerät wird automatisch neu gestartet.

WPS- oder AOSS™-Menü des Funktionstastenfeldes für die Wireless-Netzwerkkonfiguration des Gerätes verwenden (Auto-Wireless-Methode)

Wenn Ihr WLAN Access Point/Router Wi-Fi Protected Setup (PBC [1]) oder AOSS™ unterstützt, können Sie das Gerät auch einfach konfigurieren, ohne die Einstellungen Ihres Wireless-Netzwerkes zu kennen. Ihr Brother-Gerät verfügt dazu über die WPS/AOSS™-Funktion im Menü des Funktionstastenfeldes. Weitere Informationen finden Sie in der *Installationsanleitung*.

[1] Push Button Configuration (Konfiguration per Tastendruck)

Setup-Assistenten über das Funktionstastenfeld verwenden

Sie können Ihr Gerät mit Hilfe der Funktion `Setup-Assist.` konfigurieren. Diese Funktion ist im `Netzwerk`-Menü des Gerätes enthalten.

- Wenn Sie Ihr Gerät für ein kleineres Wireless-Netzwerk konfigurieren, wie zum Beispiel in Ihrem Heimbereich.
  - Um Ihr Gerät für ein vorhandenes Wireless-Netzwerk mit SSID und Netzwerkschlüssel (falls notwendig) zu konfigurieren lesen Sie die *Installationsanleitung*.
  - Wenn Ihr WLAN Access Point/Router so eingestellt ist, dass er den SSID-Name nicht rundsendet, lesen Sie *Konfiguration des Gerätes, wenn die SSID nicht rundgesendet wird* auf Seite 17.
- Wenn Sie Ihr Gerät für ein Wireless-Netzwerk konfigurieren, das IEEE 802.1x unterstützt, lesen Sie *Gerät für ein Wireless-Firmennetzwerk konfigurieren* auf Seite 20.
- Wenn Sie Ihr Gerät mit dem Wi-Fi Protected Setup (PIN-Verfahren) konfigurieren, lesen Sie *PIN-Verfahren des Wi-Fi Protected Setup verwenden* auf Seite 24.

Konfiguration des Gerätes, wenn die SSID nicht rundgesendet wird

1. Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.

   Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

Netzwerkname: (SSID, ESSID)

Kommunikationsmodus	**Authentifizierungsmethode**	**Verschlüsselungsmodus**	**Netzwerkschlüssel**
Infrastruktur	Open System	Keine	—
		WEP	
	Shared Key (freigegebener Schlüssel)	WEP	
	WPA/WPA2-PSK	AES	
		TKIP [1]	
Ad-hoc	Open System	Keine	—
		WEP	

[1] TKIP wird nur für WPA-PSK unterstützt.

Zum Beispiel:

Netzwerkname: (SSID, ESSID)
HELLO

Kommunikationsmodus	**Authentifizierungsmethode**	**Verschlüsselungsmodus**	**Netzwerkschlüssel**
Infrastruktur	WPA2-PSK	AES	12345678



Hinweis

Wenn Ihr Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Ihr Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.

2. Drücken Sie **+** oder **-**, um `Netzwerk` zu wählen.
Drücken Sie **OK**.

3. Drücken Sie **+** oder **-**, um `WLAN` zu wählen.
Drücken Sie **OK**.

4. Drücken Sie **+** oder **-**, um `Setup-Assist.` zu wählen.
Drücken Sie **OK**.

5. Wenn `WLAN aktiv?` angezeigt wird, drücken Sie **+** zur Bestätigung.
Dies startet den Wireless Setup-Assistenten.
Zum Abbrechen drücken Sie **Cancel**.

6. Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf.
Wählen Sie `<Neue SSID>` mit **+** oder **-**.
Drücken Sie **OK**.

7. Geben Sie den SSID-Namen ein. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.)
Drücken Sie **OK**.

8. Drücken Sie **+** oder **-**, um `Ad-hoc` oder `Infrastruktur` zu wählen, wenn die entsprechende Aufforderung angezeigt wird.
Drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie `Ad-hoc` gewählt haben, gehen Sie zu Schritt ❿.
Wenn Sie `Infrastruktur` gewählt haben, gehen Sie zu Schritt ❾.

9. Wählen Sie mit **+** oder **-** die Authentifizierungsmethode und drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie `Open System` gewählt haben, gehen Sie zu Schritt ❿.
Wenn Sie `Shared Key` gewählt haben, gehen Sie zu Schritt ⓫.
Wenn Sie `WPA/WPA2-PSK` gewählt haben, gehen Sie zu Schritt ⓬.

10. Wählen Sie die Verschlüsselungsmethode `Keine` oder `WEP` mit **+** oder **-** und drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie `Keine` gewählt haben, gehen Sie zu Schritt ⓮.
Wenn Sie `WEP` gewählt haben, gehen Sie zu Schritt ⓫.

11. Geben Sie den WEP-Schlüssel ein, den Sie in Schritt ❶ notiert haben. Drücken Sie **OK**. Gehen Sie zu Schritt ⓮. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.)

12. Wählen Sie die Verschlüsselungsmethode `TKIP` oder `AES` mit **+** oder **-**. Drücken Sie **OK**. Gehen Sie zu Schritt ⓭.

⑬ Geben Sie den WEP-Schlüssel ein, den Sie in Schritt ❶ notiert haben, und drücken Sie **OK**. Gehen Sie zu Schritt ⓮. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.)

⑭ Um die Einstellungen zu übernehmen, wählen Sie `Ja`. Zum Abbrechen wählen Sie `Nein`.
Sie haben folgende Möglichkeiten:
Wenn Sie `Ja` gewählt haben, gehen Sie zu Schritt ⓯.
Wenn Sie `Nein` gewählt haben, gehen Sie zurück zu Schritt ❻.

⑮ Das Gerät beginnt nun, die Verbindung mit dem von Ihnen gewählten Wireless-Gerät aufzubauen.

⑯ Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display `Verbunden` angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode und lesen Sie Problemlösung in der *Installationsanleitung*.



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation des Druckertreibers fortfahren möchten, wählen Sie Druckertreiber installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie „Start Here OSX“ im Menü der CD-ROM.

Gerät für ein Wireless-Firmennetzwerk konfigurieren

1. Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.

   Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

Netzwerkname: (SSID, ESSID)

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

Zum Beispiel:

Netzwerkname: (SSID, ESSID)
HELLO

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	EAP-FAST/MS-CHAPv2	AES	Brother	12345678



Hinweis

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, den Namen des Zertifikates zu notieren, das Sie verwenden möchten. Zur Installation des Zertifikates lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.
- Wenn Sie Ihr Gerät mit dem allgemeinen Namen des Server-Zertifikates verifizieren, empfehlen wir, den allgemeinen Namen zu notieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bei Fragen zum allgemeinen Namen des Server-Zertifikates an Ihren Netzwerkadministrator.

2. Drücken Sie **+** oder **-**, um `Netzwerk` zu wählen.
   Drücken Sie **OK**.

3. Drücken Sie **+** oder **-**, um `WLAN` zu wählen.
   Drücken Sie **OK**.

4. Drücken Sie **+** oder **-**, um `Setup-Assist.` zu wählen.
   Drücken Sie **OK**.

5. Wenn `WLAN aktiv?` angezeigt wird, drücken Sie **+** zur Bestätigung.
   Dies startet den Wireless Setup-Assistenten.
   Zum Abbrechen drücken Sie **Cancel**.

6. Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf.
   Darunter sollte die SSID sein, die Sie zuvor notiert haben. Wenn das Gerät mehr als ein Wireless-Netzwerk findet, wählen Sie mit **+** oder **-** Ihr Netzwerk aus und drücken Sie dann **OK**. Gehen Sie zu Schritt ❿.
   Wenn der Access Point so eingestellt ist, dass er keine SSID sendet, müssen Sie den SSID-Namen manuell hinzufügen. Gehen Sie zu Schritt ❼.

7. Wählen Sie `<Neue SSID>` mit **+** oder **-**.
   Drücken Sie **OK**. Gehen Sie zu Schritt ❽.

8. Geben Sie den SSID-Namen ein. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.)
   Drücken Sie **OK**. Gehen Sie zu Schritt ❾.

9. Drücken Sie **+** oder **-**, um `Infrastruktur` zu wählen, wenn die entsprechende Aufforderung angezeigt wird.
   Drücken Sie **OK**.

⑩ Wählen Sie mit **+** oder **-** die Authentifizierungsmethode und drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie `LEAP` gewählt haben, gehen Sie zu Schritt ⑯.
Wenn Sie `EAP-FAST` gewählt haben, gehen Sie zu Schritt ⑪.
Wenn Sie `PEAP` gewählt haben, gehen Sie zu Schritt ⑪.
Wenn Sie `EAP-TTLS` gewählt haben, gehen Sie zu Schritt ⑪.
Wenn Sie `EAP-TLS` gewählt haben, gehen Sie zu Schritt ⑫.

⑪ Wählen Sie die innere Authentifizierungsmethode `KEINE`, `CHAP`, `MS-CHAP`, `MS-CHAPv2`, `GTC` oder `PAP` mit **+** oder **-** und drücken Sie dann **OK**.
Gehen Sie zu Schritt ⑫.



Hinweis

Je nach verwendeter Authentifizierung unterscheiden sich die Methoden zur inneren Authentifizierung.

⑫ Wählen Sie die Verschlüsselungsmethode `TKIP` oder `AES` mit **+** oder **-** und drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie als Authentifizierungsmethode EAP-TLS verwenden, gehen Sie zu Schritt ⑬.
Wenn Sie eine andere Authentifizierungsmethode verwenden, gehen Sie zu Schritt ⑭.

⑬ Das Gerät zeigt eine Liste der verfügbaren Client-Zertifikate an. Wählen Sie das Zertifikat und gehen Sie zu Schritt ⑭.

⑭ Wählen Sie die Verifizierungsmethode `Keine Verifiz.`, `CA` oder `CA + Server-ID` mit **+** oder **-** und drücken Sie **OK**.
Sie haben folgende Möglichkeiten:
Wenn Sie `CA + Server-ID` gewählt haben, gehen Sie zu Schritt ⑮.
Wenn Sie eine andere Auswahl getroffen haben, gehen Sie zu Schritt ⑯.

Hinweis

Wenn Sie kein CA-Zertifikat importiert haben, zeigt das Gerät `Keine Verifiz.` an. Informationen zum Importieren eines CA-Zertifikates finden Sie unter *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.

⑮ Geben Sie die Server-ID ein. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.) Gehen Sie zu Schritt ⑯.

16 Geben Sie die Benutzer-ID ein, die Sie in Schritt 1 notiert haben. Drücken Sie **OK**. (Informationen, wie Sie Text eingeben können, finden Sie in der *Installationsanleitung*.)
Sie haben folgende Möglichkeiten:
Wenn Sie als Authentifizierungsmethode EAP-TLS verwenden, gehen Sie zu Schritt 18.
Wenn Sie eine andere Authentifizierungsmethode verwenden, gehen Sie zu Schritt 17.

17 Geben Sie das Kennwort ein, das Sie in Schritt 1 notiert haben. Drücken Sie **OK**. Gehen Sie zu Schritt 18.

18 Um die Einstellungen zu übernehmen, wählen Sie `Ja`. Zum Abbrechen wählen Sie `Nein`.
Sie haben folgende Möglichkeiten:
Wenn Sie `Ja` gewählt haben, gehen Sie zu Schritt 19.
Wenn Sie `Nein` gewählt haben, gehen Sie zurück zu Schritt 6.

19 Das Gerät beginnt nun, die Verbindung mit dem von Ihnen gewählten Wireless-Netzwerk aufzubauen.

20 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display `Verbunden` angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode und lesen Sie Problemlösung in der *Installationsanleitung*.



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation des Druckertreibers fortfahren möchten, wählen Sie Druckertreiber installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie „Start Here OSX“ im Menü der CD-ROM.

Gerät mit dem Brother-Installationsprogramm auf der CD-ROM für ein Wireless-Netzwerk konfigurieren

Zur Installation lesen Sie *Wireless-Konfiguration mit dem Brother-Installationsprogramm (für HL-4570CDW(T))* auf Seite 26.

PIN-Verfahren des Wi-Fi Protected Setup verwenden

Falls Ihr WLAN Access Point/Router das Wi-Fi Protected Setup (PIN-Verfahren) unterstützt, können Sie Ihr Gerät einfach konfigurieren. Das PIN-Verfahren (Personal Identification Number) ist eine von der Wi-Fi Alliance® entwickelte Verbindungsmethode. Das Wireless-Netzwerk und die Sicherheitseinstellungen können durch Übermittlung einer PIN, die von Ihrem Gerät (dem „Antragsteller“) erstellt wurde, an den Registrar (dem Gerät zum Verwalten des Wireless LANs) eingerichtet werden. Informationen zur Verwendung des Wi-Fi Protected Setup finden Sie im Benutzerhandbuch Ihres WLAN Access Points/Routers.



Hinweis

Auf Routern oder Access Points, die Wi-Fi Protected Setup unterstützen, finden Sie ein Symbol, wie unten gezeigt.



1. Drücken Sie **+** oder **-**, um `Netzwerk` zu wählen.
2. Drücken Sie **+** oder **-**, um `WLAN` zu wählen.
3. Drücken Sie **+** oder **-**, um `WPS + PIN-Code` zu wählen.
4. Im Display wird eine 8-stellige PIN angezeigt und das Gerät beginnt, 5 Minuten lang nach einem WLAN Access Point/Router zu suchen.
5. Öffnen Sie auf einem Computer in Ihrem Netzwerk einen Browser und geben Sie “`http://access point’s IP address/`” ein. (Wobei “`access point’s IP address`” die IP-Adresse des Gerätes ist, das als Registrar [1] verwendet wird.)Gehen Sie zur Einstellungsseite für WPS (Wi-Fi Protected Setup), geben Sie die in Schritt ❹ im Display angezeigte PIN für den Registrar ein und folgen Sie dann den Anweisungen auf dem Bildschirm.

[1] Der Registrar ist in der Regel der WLAN Access Point/Router.



Hinweis

Die Einstellungsseite unterscheidet sich je nach WLAN Access Point/Router. Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde.

Windows Vista®/Windows® 7

Falls Sie Ihren Computer als Registrar verwenden, gehen Sie wie folgt vor:



Hinweis

- Um einen Computer mit Windows Vista® oder Windows® 7als Registrar zu verwenden, muss dieser zuvor in Ihrem Netzwerk registriert werden. Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde.
- Wenn Sie Windows® 7 als Registrar verwenden, können Sie nach der Wireless-Konfiguration den Druckertreiber mit Hilfe der Anweisungen auf dem Bildschirm installieren. Wenn Sie das gesamte Treiber- und Software-Paket installieren möchten, folgen Sie zur Installation den Schritten in der *Installationsanleitung*.

1 (Windows Vista®)
Klicken Sie auf die Schaltfläche und dann auf **Netzwerk**.
(Windows® 7)
Klicken Sie auf die Schaltfläche und dann auf **Geräte und Drucker**.

2 (Windows Vista®)
Klicken Sie auf **Ein Drahtlosgerät hinzufügen**.
(Windows® 7)
Klicken Sie auf **Geräte hinzufügen**.

3 Wählen Sie Ihr Gerät und klicken Sie auf **Weiter**.

4 Geben Sie die PIN ein, die das Display in Schritt ❹ angezeigt hat, und klicken Sie dann auf **Weiter**.

5 Wählen Sie das Netzwerk, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie dann auf **Weiter**.

6 Klicken Sie auf **Schließen**.

6 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display `Verbunden` angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode und lesen Sie Problemlösung in der *Installationsanleitung*.



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation des Druckertreibers fortfahren möchten, wählen Sie Druckertreiber installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie „Start Here OSX“ im Menü der CD-ROM.



Wireless-Konfiguration mit dem Brother-Installationsprogramm (für HL-4570CDW(T))

Vor dem Konfigurieren der Wireless-Einstellungen

WICHTIG

- Mit der folgenden Anleitung können Sie Ihr Brother-Gerät mit dem Brother-Installationsprogramm in einer Netzwerkumgebung installieren. Dieses Programm finden Sie auf der CD-ROM, die mit Ihrem Gerät geliefert wurde.
- Sie können Ihr Brother-Gerät auch mit WPS oder AOSS™ über das Funktionstastenfeld einrichten (empfohlenes Verfahren). Informationen dazu finden Sie in der mitgelieferten *Installationsanleitung*.
- Falls Sie die Wireless-Einstellungen des Gerätes zuvor schon einmal konfiguriert haben, müssen Sie erst die Netzwerkeinstellungen (LAN) zurücksetzen, bevor Sie die Wireless-Einstellungen erneut konfigurieren können. Drücken Sie **+** oder **-**, um `Netzwerk`, `Netzwerk-Reset`, `Reset` zu wählen, und wählen Sie dann `Ja`, um die Änderung zu bestätigen. Das Gerät wird automatisch neu gestartet.
- Wenn Sie die Windows®-Firewall oder die Firewall-Funktion einer Anti-Spyware oder Antivirus-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, aktivieren Sie die Firewall bitte wieder.
- Sie benötigen zum Konfigurieren vorübergehend ein USB-Kabel oder ein Ethernetkabel.
- **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**

  Notieren Sie sich die aktuellen Einstellungen, wie die SSID und die in Ihrer Netzwerkumgebung verwendete Methode zur Authentifizierung und Verschlüsselung. Falls Sie diese Einstellungen nicht kennen, wenden Sie sich an Ihren Netzwerkadministrator oder an den Hersteller Ihres WLAN Access Points/Routers.

Wireless-Einstellungen konfigurieren

1. Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.
   Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

   Für die Konfiguration eines privaten Wireless-Netzwerkes

   Wenn Sie Ihr Gerät für ein kleineres Wireless-Netzwerk konfigurieren, wie zum Beispiel in Ihrem Heimbereich, notieren Sie Ihre SSID und den Netzwerkschlüssel.

Netzwerkname (SSID, ESSID)	Netzwerkschlüssel

Zum Beispiel:

Netzwerkname (SSID, ESSID)	Netzwerkschlüssel
HELLO	12345678

Für die Konfiguration eines Wireless-Firmennetzwerk

Wenn Sie Ihr Gerät für ein Wireless-Netzwerk konfigurieren, das IEEE 802.1x unterstützt, notieren Sie Ihre Authentifizierungsmethode, Verschlüsselungsmethode, Benutzer-ID und das Kennwort.

Netzwerkname: (SSID, ESSID)

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

Zum Beispiel:

Netzwerkname: (SSID, ESSID)
HELLO

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	EAP-FAST/MS-CHAPv2	AES	Brother	12345678



Hinweis

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, den Namen des Zertifikates zu notieren, das Sie verwenden möchten. Zur Installation des Zertifikates lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.
- Wenn Sie Ihr Gerät mit dem allgemeinen Namen des Server-Zertifikates verifizieren, empfehlen wir, den allgemeinen Namen zu notieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bei Fragen zum allgemeinen Namen des Server-Zertifikates an Ihren Netzwerkadministrator.

2 Legen Sie die mitgelieferte CD-ROM in das CD-ROM-Laufwerk ein.

(Windows®)

1 Der Startbildschirm wird automatisch angezeigt.

Wählen Sie Ihr Modell und die Sprache.

2 Das Hauptmenü der CD-ROM wird angezeigt. Klicken Sie auf **Druckertreiber installieren**.



Hinweis

- Falls dieses Fenster nicht erscheint, führen Sie über den Windows®-Explorer das Programm Start.exe im Hauptverzeichnis der Brother CD-ROM aus.
- Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird:
  (Windows Vista®) Klicken Sie auf **Zulassen**.
  (Windows® 7) Klicken Sie auf **Ja**.

3 Wenn die **Lizenzvereinbarung** erscheint, klicken Sie auf **Ja**, wenn Sie die Lizenzvereinbarung akzeptieren.

4 Wählen Sie **Drahtlose Netzwerkverbindung (Wireless LAN)** und klicken Sie dann auf **Weiter**.

5 Wählen Sie **Brother Peer-to-Peer Netzwerkdrucker** oder **Über das Netzwerk gemeinsam benutzter Drucker** und klicken Sie dann auf **Weiter**.

6 Wenn Sie **Über das Netzwerk gemeinsam benutzter Drucker** gewählt haben, wählen Sie die Warteschlange Ihres Gerätes auf dem Bildschirm **Drucker suchen** und klicken Sie dann auf **OK**.



Hinweis

Wenden Sie sich bitte an Ihren Administrator, falls Sie den Standort oder den Namen des Gerätes im Netzwerk nicht kennen.

7 Wählen Sie die Option für die Firewall-Einstellung auf dem Bildschirm **Firewall/Antiviren-Programm gefunden** und klicken Sie dann auf **Weiter**.

(Macintosh)

1 Der Startbildschirm wird automatisch angezeigt. Klicken Sie auf **Start Here OSX**. Wählen Sie Ihr Gerät und klicken Sie auf **Weiter**.

2 Wählen Sie **Drahtlose Netzwerkverbindung (Wireless LAN)** und klicken Sie dann auf **Weiter**.

3 Wählen Sie **Ja, mein Access Point unterstützt WPS oder AOSS und ich möchte diese verwenden.** oder **Nein** und klicken Sie dann auf **Weiter**.
Wenn Sie **Nein** gewählt haben, haben Sie vier verschiedene Möglichkeiten, die Wireless-Einstellung zu konfigurieren.

- Vorübergehend ein USB-Kabel verwenden
- Vorübergehend ein Ehternetkabel (LAN) verwenden
- Manuelle Konfiguration über das Funktionstastenfeld
- Ad-hoc-Modus verwenden



Hinweis

Für Nutzer des Ad-hoc-Modus:

- Wenn nach dem Ändern der Wireless-Einstellungen eine Meldung zum Neustart des Computers auffordert, starten Sie den Computer neu. Gehen Sie dann zurück zu Schritt 2.
- Sie können die Wireless-Einstellungen Ihres Computers vorübergehend ändern.

(Windows Vista® und Windows® 7)

1 Klicken Sie auf die Schaltfläche und dann auf **Systemsteuerung**.

2 Klicken Sie auf **Netzwerk und Internet** und dann auf das Symbol **Netzwerk-und Freigabecenter**.

3 Klicken Sie auf **Verbindung mit einem Netzwerk herstellen**.

4 In der Liste wird der SSID-Name Ihres Wireless-Gerätes angezeigt. Wählen Sie **SETUP** und klicken Sie dann auf **Verbindung herstellen**.

5 (Nur für Windows Vista®)
Klicken Sie auf **Trotzdem verbinden** und dann auf **Schließen**.

6 (Windows Vista®)
Klicken Sie auf **Status anzeigen** unter **Drahtlosnetzwerkverbindung (SETUP)**.

7 (Windows® 7)
Klicken Sie auf **Drahtlosnetzwerkverbindung (SETUP)**.

8 Klicken Sie auf **Details…** und überprüfen Sie die **Netzwerkverbindungsdetails**. Es kann einige Minuten dauern, bis die IP-Adresse von 0.0.0.0 zu 169.254.x.x geändert und am Bildschirm angezeigt wird (x.x steht jeweils für eine Zahl von 1 bis 254).

(Windows® XP SP2)

1 Klicken Sie auf **Start** und dann auf **Systemsteuerung**.

2 Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen**.

3 Klicken Sie auf das Symbol **Netzwerkverbindungen**.

4 Klicken Sie mit der rechten Maustaste auf **Drahtlose Netzwerkverbindung**. Klicken Sie auf **Verfügbare drahtlose Netzwerke anzeigen**.

5 In der Liste wird der SSID-Name Ihres Wireless-Druckers angezeigt. Wählen Sie **SETUP** und klicken Sie auf **Verbindung herstellen**.

6 Überprüfen Sie den Status der **Drahtlosen Netzwerkverbindung**. Es kann einige Minuten dauern, bis die IP-Adresse von 0.0.0.0 zu 169.254.x.x geändert und am Bildschirm angezeigt wird (x.x steht jeweils für eine Zahl von 1 bis 254).

(Macintosh)

1 Klicken Sie in der Menüleiste auf das AirPort-Statussymbol.

2 Wählen Sie **SETUP** im Popup-Menü.

3 Nun ist die Verbindung zu Ihrem Wireless-Netzwerk hergestellt.

---

4 Folgen Sie den Anweisungen auf dem Bildschirm, um die Wireless-Einstellungen zu konfigurieren.



Nachdem Sie die Wireless-Einstellungen abgeschlossen haben, können Sie mit der Installation der Druckertreiber fortfahren. Klicken Sie im Installationsdialogfeld auf Weiter und folgen Sie den Anweisungen auf dem Bildschirm.

5 Einstellungen über das Funktionstastenfeld

Netzwerk-Menü

Über das Netzwerk-Menü des Funktionstastenfeldes können Sie das Brother-Gerät entsprechend Ihrer Netzwerkkonfiguration einrichten. (Weitere Informationen zur Verwendung des Funktionstastenfeldes finden Sie im *Benutzerhandbuch*.) Drücken Sie eine der Menü-Tasten (**+**, **-**, **OK** oder **Back**), um das Hauptmenü aufzurufen. Drücken Sie dann **+** oder **-**, um Netzwerk zu wählen. Rufen Sie nun die Menüauswahl auf, die Sie konfigurieren möchten. (Weitere Informationen zum Menü finden Sie unter *Funktionstabelle und werkseitige Standardeinstellungen* auf Seite 37.)

Hinweis: Das Gerät wird mit dem Dienstprogramm BRAdmin Light oder mit der Anwendung Web Based Management ausgeliefert, die zum Konfigurieren vieler Netzwerkeinstellungen genutzt werden können. (Siehe *Andere Verwaltungsprogramme* auf Seite 6.)

TCP/IP

Wenn Sie das Gerät mit einem Netzwerkkabel an das Netzwerk anschließen, verwenden Sie die Einstellungen im Menü LAN (Kabel). Wenn Sie das Gerät mit einem Wireless Ethernet-Netzwerk verbinden, verwenden Sie die Einstellungen im Menü WLAN.

Boot-Methode

Mit dieser Funktion wird festgelegt, wie das Gerät eine IP-Adresse erhält.

Einstellung „Auto“

Wenn diese Einstellung gewählt ist, sucht das Gerät im Netzwerk nach einem DHCP-Server. Wenn ein DHCP-Server erreicht werden kann und dieser so konfiguriert ist, dass er dem Gerät eine IP-Adresse zuweisen kann, wird die vom DHCP-Server zugewiesene IP-Adresse verwendet. Kann kein DHCP-Server gefunden werden, sucht das Gerät nach einem BOOTP-Server. Wenn ein BOOTP-Server erreichbar und entsprechend konfiguriert ist, weist dieser dem Gerät eine IP-Adresse zu. Ist kein BOOTP-Server erreichbar, sucht das Gerät nach einem RARP-Server. Wenn auch kein RARP-Server antwortet, wird die IP-Adresse über APIPA ermittelt. Nach dem ersten Einschalten des Gerätes kann die Suche des Gerätes nach einem Server im Netzwerk einige Minuten dauern.

Einstellung „Statisch“

Mit dieser Einstellung muss die IP-Adresse des Gerätes manuell zugewiesen werden. Die IP-Adresse ist dann auf die hier gespeicherte Adresse festgelegt.



Hinweis

Wenn Sie Ihren PrintServer nicht über DHCP, BOOTP oder RARP konfigurieren möchten, stellen Sie die BOOT-Methode auf Statisch ein, damit der PrintServer eine feste IP-Adresse erhält. Dies verhindert, dass der PrintServer versucht, eine IP-Adresse von einem dieser Systeme zu erhalten. Um die Boot-Methode zu ändern, verwenden Sie das Funktionsmenü Ihres Gerätes, das Dienstprogramm BRAdmin Light oder das Web Based Management.

IP-Adresse

Dieses Feld zeigt die aktuelle IP-Adresse des Gerätes an. Wenn Sie die `BOOT-Methode Statisch` gewählt haben, geben Sie die IP-Adresse ein, die Sie diesem Gerät zuweisen möchten (fragen Sie Ihren Netzwerkadministrator nach der zu verwendenden IP-Adresse). Falls Sie eine andere Boot-Methode als `Statisch` gewählt haben, versucht das Gerät, eine IP-Adresse über das DHCP- oder BOOTP-Protokoll zu beziehen. Die werkseitig eingestellte IP-Adresse Ihres Gerätes ist wahrscheinlich nicht mit dem Nummerierungssystem in Ihrem Netzwerk kompatibel. Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach einer gültigen IP-Adresse für das Gerät in Ihrem Netzwerk.

Subnetzmaske

Dieses Feld zeigt die aktuelle Subnetzmaske des Gerätes an. Wenn die Subnetzmaske nicht automatisch über DHCP oder BOOTP zugewiesen wird, tragen Sie hier die gewünschte Subnetzmaske ein. Fragen Sie Ihren Netzwerkadministrator nach einer gültigen Subnetzmaske für das Gerät.

Gateway

Dieses Feld zeigt die aktuelle Gateway- oder Router-Adresse des Gerätes an. Wenn die Gateway- oder Router-Adresse nicht automatisch über DHCP oder BOOTP zugewiesen wird, tragen Sie hier die gewünschte Adresse ein. Lassen Sie dieses Feld leer, wenn Sie weder Gateway noch Router verwenden. Fragen Sie gegebenenfalls Ihren Netzwerkadministrator.

IP-Bootversuche

Dieses Feld zeigt an, wie oft das Gerät über die von Ihnen eingestellte Boot-Methode nach einer IP-Adresse im Netzwerk sucht. (Siehe *Boot-Methode* auf Seite 31.)

APIPA

Wenn diese Einstellung aktiviert ist (`Ein`), weist der PrintServer automatisch eine IP-Adresse aus dem Bereich von 169.254.1.0 bis 169.254.254.255 zu, falls er die IP-Adresse nicht über die eingestellte Boot-Methode erhalten kann. (Siehe *Boot-Methode* auf Seite 31.) Ist diese Option deaktiviert (`Aus`), bleibt die IP-Adresse unverändert, falls der PrintServer keine IP-Adresse über die eingestellte Boot-Methode erhalten kann.

IPv6

Dieses Gerät ist kompatibel mit IPv6, der nächsten Generation der Internetprotokolle. Wenn Sie das IPv6-Protokoll verwenden möchten, wählen Sie `Ein`. Die Standardeinstellung für IPv6 ist `Aus`. Weitere Informationen zum IPv6-Protokoll erhalten Sie unter http://solutions.brother.com/.



Hinweis

- Wenn Sie IPv6 auf `Ein` eingestellt haben, schalten Sie das Gerät aus und wieder ein, um dieses Protokoll zu aktivieren.
- Nachdem Sie für IPv6 `Ein` gewählt haben, gilt diese Einstellung sowohl für den verkabelten LAN-Anschluss als auch für den WLAN-Anschluss.

Ethernet (nur verkabeltes Netzwerk)

Ethernet-Link-Modus: Mit der Einstellung „Auto“ kann der PrintServer im 100BASE-TX oder 10BASE-T Voll- oder Halbduplex-Modus mit automatischer Verständigung (Auto Negotiation) betrieben werden.



Hinweis

Wenn hier nicht die richtige Einstellung gewählt ist, kann nicht mit dem PrintServer kommuniziert werden.

Status (für HL-4140CN und HL-4150CDN)/Status (verkabelt) (für HL-4570CDW(T))

Dieses Feld zeigt den aktuellen Status des verkabelten Netzwerkes an.

Setup-Assistent (nur für Wireless-Netzwerke)

Der `Setup-Assist.` führt Sie durch die Konfiguration des Wireless-Netzwerkes. (Weitere Informationen finden Sie in der *Installationsanleitung* oder unter *Setup-Assistenten über das Funktionstastenfeld verwenden* auf Seite 16.)

WPS oder AOSS™ (nur für Wireless-Netzwerke)

Wenn Ihr WLAN Access Point/Router das Wi-Fi Protected Setup (PBC [1]) oder AOSS™ (Auto-Wireless-Modus) unterstützt, können Sie das Gerät auch ohne Computer einfach konfigurieren. (Weitere Informationen finden Sie in der *Installationsanleitung* oder unter *WPS- oder AOSS™-Menü des Funktionstastenfeldes für die Wireless-Netzwerkkonfiguration des Gerätes verwenden (Auto-Wireless-Methode)* auf Seite 16.)

[1] Push Button Configuration (Konfiguration per Tastendruck)

WPS mit PIN-Code (nur für Wireless-Netzwerke)

Falls Ihr WLAN Access Point/Router das Wi-Fi Protected Setup (PIN-Verfahren) unterstützt, können Sie Ihr Gerät auch ohne Computer einfach konfigurieren. (Weitere Informationen finden Sie unter *PIN-Verfahren des Wi-Fi Protected Setup verwenden* auf Seite 24.)

WLAN-Status (nur für Wireless-Netzwerke)

Status

Dieses Feld zeigt den aktuellen Status des Wireless-Netzwerkes an.

Signal

Dieses Feld zeigt die aktuelle Signalstärke des Wireless-Netzwerkes an.

Kanal

Dieses Feld zeigt den aktuellen Kanal des Wireless-Netzwerkes an.

Geschwindigkeit

Dieses Feld zeigt die aktuelle Geschwindigkeit des Wireless-Netzwerkes an.

SSID

Dieses Feld zeigt die aktuelle SSID des Wireless-Netzwerkes an. Das Display zeigt bis zu 32 Zeichen des SSID-Namens an.

Komm.-Modus

Dieses Feld zeigt den aktuellen Kommunikationsmodus des Wireless-Netzwerkes an.

MAC-Adresse

Die MAC-Adresse ist eine eindeutige Zahl, die der Netzwerkschnittstelle des Gerätes zugeordnet wird. Sie können die MAC-Adresse Ihres Gerätes über das Funktionstastenfeld des Gerätes überprüfen.

Werkseinstellungen (für HL-4570CDW(T))

Mit der Funktion `Werkseinstell.` können Sie die Netzwerkeinstellungen für das verkabelte oder das Wireless-Netzwerk auf die werkseitigen Standardeinstellungen zurücksetzen. Wenn Sie sowohl die Einstellungen für das verkabelte als auch die Einstellungen für das Wireless-Netzwerk zurücksetzen möchten, lesen Sie *Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen zurücksetzen* auf Seite 35.

Verkabelt aktiv (für HL-4570CDW(T))

Wenn Sie eine verkabelte Netzwerkverbindung verwenden möchten, wählen Sie für `Verkabelt akt.` die Einstellung `Ein`.

WLAN aktiv (für HL-4570CDW(T))

Wenn Sie eine Wireless-Netzwerkverbindung verwenden möchten, wählen Sie für `WLAN aktiv` die Einstellung `Ein`.



Hinweis

Wenn Ihr Gerät mit einem Netzwerkkabel verbunden ist, wählen Sie für `Verkabelt akt.` die Einstellung `Aus`.

Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen zurücksetzen

Sie können den PrintServer (d. h. alle Einstellungen wie Kennwort und IP-Adresse) auf die werkseitigen Standardeinstellungen zurücksetzen.

Hinweis

- Diese Funktion setzt alle Einstellungen für verkabelte und Wireless-Netzwerke auf die werkseitigen Standardeinstellungen zurück.
- Sie können den PrintServer auch mit Hilfe der BRAdmin-Anwendungen oder dem Web Based Management auf die werkseitigen Standardeinstellungen zurücksetzen. (Weitere Informationen finden Sie unter *Andere Verwaltungsprogramme* auf Seite 6.)

1. Drücken Sie **+** oder **-**, um `Netzwerk` zu wählen.
   Drücken Sie **OK**.
2. Drücken Sie **+** oder **-**, um `Netzwerk-Reset` zu wählen.
   Drücken Sie **OK**.
3. Drücken Sie **+**, um `Reset` zu wählen.
4. Drücken Sie **+**, um `Ja` für einen Neustart zu wählen.
5. Das Gerät wird neu gestartet.

Netzwerk-Konfigurationsliste drucken

Hinweis

Knotenname: Den Knotennamen können Sie der Netzwerk-Konfigurationsliste entnehmen. Der Standardknotenname ist “BRNxxxxxxxxxxxx” für ein verkabeltes Netzwerk und “BRWxxxxxxxxxxxx” für ein Wireless-Netzwerk . (“xxxxxxxxxxxx” steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

Die Netzwerk-Konfigurationsliste ist eine Liste aller aktuellen Netzwerk-Konfigurationseinstellungen einschließlich der Netzwerkeinstellungen Ihres PrintServers.

1. Drücken Sie **+** oder **-**, um `Geräte-Info` zu wählen.
   Drücken Sie **OK**.
2. Drücken Sie **+** oder **-**, um `Netzeinst.druck` zu wählen.
   Drücken Sie **OK**.



Hinweis

Wenn als **IP Address** in der Netzwerk-Konfigurationsliste die Angabe **0.0.0.0** ausgedruckt wurde, warten Sie eine Minute und wiederholen Sie dann den Vorgang.

WLAN-Bericht drucken (für HL-4570CDW(T))

Die Funktion `WLAN-Bericht dr.` druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Wireless-Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode und lesen Sie Problemlösung in der *Installationsanleitung*.

1. Drücken Sie **+** oder **-**, um `Geräte-Info` zu wählen.
   Drücken Sie **OK**.
2. Drücken Sie **+** oder **-**, um `WLAN-Bericht dr.` zu wählen.
   Drücken Sie **OK**.

Funktionstabelle und werkseitige Standardeinstellungen

HL-4140CN und HL-4150CDN

Die werkseitigen Einstellungen sind fettgedruckt und mit einem Sternchen markiert.

Hauptmenü	Untermenü	Menüauswahl	Optionen
Netzwerk	TCP/IP	BOOT-Methode	**Auto***/Statisch/RARP/BOOTP/DHCP
		IP-Adresse	**(000.000.000.000)*** [1]
		Subnet-Mask	**(000.000.000.000)*** [1]
		Gateway	**(000.000.000.000)*** [1]
		IP-Boot-Versuche	0/1/2/**3***.../32767
		APIPA	**Ein***/Aus
		IPv6	**Aus***/Ein
	Ethernet		**Auto***/100B-FD/100B-HD/10B-FD/10B-HD
	Status		Aktiv 100B-FD/Aktiv 100B-HD/ Aktiv 10B-FD/Aktiv 10B-HD/Inaktiv
	MAC-Adresse		
	Netzwerk-Reset	Setzt alle Netzwerkeinstellungen des internen PrintServers auf die werkseitigen Standardeinstellungen zurück.	

[1] Beim Verbinden mit dem Netzwerk stellt das Gerät IP-Adresse und Subnetzmaske automatisch auf Werte ein, die für Ihr Netzwerk geeignet sind.

5

HL-4570CDW(T)

Die werkseitigen Einstellungen sind fettgedruckt und mit einem Sternchen markiert.

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk	LAN (Kabel)	TCP/IP	BOOT-Methode	**Auto***/Statisch/RARP/BOOTP/DHCP
			IP-Adresse	(000.000.000.000)*[1]
			Subnet-Mask	(000.000.000.000)*[1]
			Gateway	(000.000.000.000)*[1]
			IP-Boot-Versuche	0/1/2/**3***.../32767
			APIPA	**Ein***/Aus
			IPv6	**Aus***/Ein
		Ethernet		**Auto***/100B-FD/100B-HD/ 10B-FD/10B-HD
		Status (verk.)		Aktiv 100B-FD/ Aktiv 100B-HD/ Aktiv 10B-FD/ Aktiv 10B-HD/Inaktiv/ Verkabelt AUS
		MAC-Adresse		
		Werkseinstell.	Setzt die Einstellungen des internen PrintServers für das verkabelte Netzwerk auf die werkseitigen Standardeinstellungen zurück.	
		Verkabelt akt.		**Ein***/Aus

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk	WLAN	TCP/IP	BOOT-Methode	**Auto***/Statisch/RARP/BOOTP/DHCP
			IP-Adresse	(000.000.000.000)* [1]
			Subnet-Mask	(000.000.000.000)* [1]
			Gateway	(000.000.000.000)* [1]
			IP-Boot-Versuche	0/1/2/**3***.../32767
			APIPA	**Ein***/Aus
			IPv6	**Aus***/Ein
		Setup-Assist.		
		WPS/AOSS		
		WPS + PIN-Code		
		WLAN-Status	Status	
			Signal	(Erscheint nur, wenn WLAN aktiv auf Ein eingestellt ist.)
			Kanal	
			Geschwindigk.	
			SSID	
			Komm.-Modus	Ad-hoc/Infrastruktur
		MAC-Adresse		
		Werkseinstell.	Setzt die Einstellungen des internen PrintServers für das Wireless-Netzwerk auf die werkseitigen Standardeinstellungen zurück.	
		WLAN aktiv		**Aus***/Ein
	Netzwerk-Reset	Setzt alle Netzwerkeinstellungen des internen PrintServers auf die werkseitigen Standardeinstellungen zurück.		

[1] Beim Verbinden mit dem Netzwerk stellt das Gerät IP-Adresse und Subnetzmaske automatisch auf Werte ein, die für Ihr Netzwerk geeignet sind.

5

6 Web Based Management

Übersicht

Sie können Ihr Gerät mit einem normalen Webbrowser über HTTP (Hyper Text Transfer Protocol) verwalten. Mit einem Browser können Sie die folgenden Informationen von einem Gerät in Ihrem Netzwerk abfragen bzw. Einstellungen vornehmen.

- Informationen über den Gerätestatus
- Netzwerkeinstellungen wie z. B. TCP/IP-Informationen ändern
- Benutzersperre 2.0 konfigurieren
- "Druckprotokoll im Netzwerk speichern" konfigurieren
- Informationen zur Software-Version von Gerät und PrintServer
- Netzwerk- und Gerätekonfiguration ändern



Hinweis

Wir empfehlen, den Microsoft® Internet Explorer® 6.0 (oder höher) oder Firefox 3.0 (oder höher) für Windows® und Safari 3.0 (oder höher) für Macintosh zu verwenden. Stellen Sie auch sicher, dass JavaScript und Cookies in dem von Ihnen benutzten Browser stets aktiviert sind. Wenn Sie andere Webbrowser verwenden, vergewissern Sie sich, dass diese mit HTTP 1.0 und HTTP 1.1 kompatibel sind.

In Ihrem Netzwerk muss das TCP/IP-Protokoll aktiviert sein und Sie müssen eine gültige IP-Adresse für den PrintServer und Ihren Computer eingerichtet haben.

Geräteeinstellungen mit dem Web Based Management (Webbrowser) konfigurieren

Sie können die Einstellungen des PrintServers über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) ändern.



Hinweis

Wir empfehlen, beim Konfigurieren der Einstellungen über das Web Based Management das HTTPS-Protokoll zum sicheren Datenaustausch über das Internet zu verwenden. Zur Verwendung des HTTPS-Protokolls lesen Sie *Netzwerkgerät mit SSL/TLS sicher verwalten* auf Seite 52.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „`http://machine's IP address/`" ein (wobei „`machine's IP address`" für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     `http://192.168.1.2/`



- Falls Sie ein Domänen-Namensystem (DNS) verwenden oder die Verwendung von NetBIOS-Namen aktiviert haben, können Sie einen anderen Namen wie zum Beispiel „Shared_Printer“ anstelle der IP-Adresse eingeben.
  - Zum Beispiel:

  `http://Shared_Printer/`

  Wenn Sie die Verwendung von NetBIOS-Namen aktiviert haben, können Sie auch den Knotennamen verwenden.
  - Zum Beispiel:

  `http://brnxxxxxxxxxxxx/`

  Den NetBIOS-Namen können Sie der Netzwerk-Konfigurationsliste entnehmen. (Zum Ausdrucken der Netzwerk-Konfigurationsliste lesen Sie *Netzwerk-Konfigurationsliste drucken* auf Seite 35.)
- Macintosh-Nutzer können einfach durch Klicken auf das Gerätesymbol im **Status Monitor**-Bildschirm auf das Web Based Management zugreifen. Weitere Informationen finden Sie im *Benutzerhandbuch*.

3. Klicken Sie auf **Netzwerkkonfiguration**.
4. Geben Sie einen Benutzernamen und ein Kennwort ein. Der Standardbenutzername ist „**admin**“ und das Standardkennwort ist „**access**“.
5. Klicken Sie auf **OK**.
6. Sie können nun die Einstellungen des PrintServers ändern.



Wenn Sie die Protokolleinstellungen geändert haben, klicken Sie auf **Senden** und starten Sie dann das Gerät neu, um die Konfiguration zu aktivieren.

Benutzersperre 2.0

Die Benutzersperre 2.0 von Brother hilft Ihnen, Geld zu sparen und die Sicherheit zu erhöhen, indem Funktionen Ihres Brother-Gerätes gesperrt werden können.

Durch die Vergabe von Benutzernamen und Kennwörtern kann nur bestimmten Personen der Zugriff auf besondere oder auf alle Funktionen ermöglicht und die Anzahl der Seiten, die gedruckt werden können, begrenzt werden. Dies bedeutet, dass Funktionen des Gerätes nur von den dazu berechtigten Personen genutzt werden können.

Sie können die folgenden Einstellungen der Benutzersperre 2.0 mit BRAdmin Professional 3 oder dem Web Based Management konfigurieren und ändern.

- **PC-Druck** [1]
- **USB-Direktdruck**
- **Farbdruck**
- **Seitenbegrenzung**
- **Seitenzähler**

[1] Durch die Registrierung von PC-Anmeldenamen der Benutzer können Sie das Drucken vom PC aus einschränken, ohne dass Benutzer ein Kennwort eingeben müssen. Weitere Informationen finden Sie unter *PC-Druck-Einschränkung durch Benutzernamen* auf Seite 43.

Einstellungen der Benutzersperre 2.0 mit dem Web Based Management (Webbrowser) konfigurieren

Grundlegende Einstellungen

1. Klicken Sie auf der Webseite Ihres Gerätes auf **Administratoreinstellungen** und dann auf **Benutzersperre**.
2. Wählen Sie **Ein** für **Benutzersperre**.
3. Geben Sie unter **ID-Nummer/Name** einen 15-stelligen alphanumerischen Gruppen- oder Benutzernamen und dann im Feld **PIN** ein vierstelliges Kennwort ein.
4. Deaktivieren Sie unter **Drucken** die Kontrollkästchen der Funktionen, die Sie sperren möchten. Wenn Sie die maximale Anzahl von Seiten, die gedruckt werden können, begrenzen möchten, aktivieren Sie das Kontrollkästchen **Ein** unter **Seitenbegrenzung** und geben Sie dann die gewünschte Anzahl im Feld **Max.** ein. Klicken Sie auf **Senden**
5. Falls Sie den PC-Druck über den PC-Anmeldenamen (Benutzernamen) einschränken möchten, klicken Sie auf **PC-Druck-Einschränkung durch Benutzernamen** und konfigurieren Sie dann die Einstellungen. (Siehe *PC-Druck-Einschränkung durch Benutzernamen* auf Seite 43.)

PC-Druck-Einschränkung durch Benutzernamen

Durch Konfiguration dieser Einstellung kann das Gerät den Benutzer anhand des PC-Anmeldenamens erkennen und darüber das Drucken von einem registrierten Computer aus erlauben.

1. Klicken Sie auf **PC-Druck-Einschränkung durch Benutzernamen**. Der Bildschirm **PC-Druck-Einschränkung durch Benutzernamen** wird angezeigt.
2. Wählen Sie **Ein** für **PC-Druck-Einschränkung**.
3. Wählen Sie die ID-Nummer, die Sie unter **ID-Nummer/Name** in Schritt ❸ unter *Grundlegende Einstellungen* eingegeben haben, nun hier in der Pulldown-Liste **ID-Nummer** für jeden Anmeldenamen aus und geben Sie dann den PC-Anmeldenamen des Benutzers in das Feld **Anmeldename** ein.
4. Klicken Sie auf **Senden**.

Hinweis

- Wenn Sie das Drucken vom PC aus (PC-Druck) für Benutzergruppen einschränken möchten, wählen Sie dieselbe ID-Nummer für jeden PC-Anmeldenamen, den Sie in die Gruppe aufnehmen möchten.
- Wenn Sie die PC-Anmeldenamen-Funktion verwenden, müssen Sie auch sicherstellen, dass das Kontrollkästchen **PC-Anmeldenamen verwenden** im Druckertreiber aktiviert ist. Weitere Informationen zum Druckertreiber finden Sie im *Benutzerhandbuch*.
- Das Drucken über den BR-Script-Treiber wird von der Benutzersperre nicht unterstützt.

Allgemeinen Benutzer einrichten

Sie können einen allgemeinen Benutzer einrichten und für diesen den Zugang festlegen, welche Funktionen verfügbar sind. Diese Einstellungen sind dann für alle Benutzer gültig, die zur Nutzung des Gerätes kein Kennwort eingeben.

1. Deaktivieren Sie neben **Allgemeiner Benutzer** das Kontrollkästchen der Funktion, die Sie sperren möchten.
2. Klicken Sie auf **Senden**.

Andere Funktionen

Sie können die folgenden Funktionen der Benutzersperre 2.0 einstellen:

- **Alle Zähler zurücksetzen**

  Sie können den Seitenzähler zurücksetzen, indem Sie auf **Alle Zähler zurücksetzen** klicken.
- **Export in CSV-Datei**

  Sie können den aktuellen Seitenzählerstand einschließlich **ID-Nummer/Name** in eine CSV-Datei exportieren.
- **Letzter Zähler-Eintrag**

  Das Gerät erhält die Seitenzahl bei, nachdem der Zähler zurückgesetzt wurde.
- **Zähler autom. zurücksetzen**

  Sie können die Seitenzähler automatisch in regelmäßigen Abständen zurücksetzen, während das Gerät eingeschaltet ist, zum Beispiel täglich, monatlich oder wöchentlich.

Mit SNTP-Server synchronisieren

SNTP ist ein Protokoll zur Synchronisation der Zeit, die vom Gerät zur Authentifizierung verwendet wird, mit der Zeit des SNTP-Zeitservers . Sie können die Zeit, die vom Gerät verwendet wird, in regelmäßigen Abständen mit der UTC-Zeit (Coordinated Universal Time) synchronisieren, die vom SNTP-Zeitserver zur Verfügung gestellt wird.



Hinweis

Diese Funktion steht nicht in allen Ländern zur Verfügung.

1. Klicken Sie auf **Netzwerkkonfiguration** und klicken Sie dann auf **Protokoll konfigurieren**.
2. Wählen Sie das Kontrollkästchen **SNTP**, um die Einstellung zu aktivieren.
3. Klicken Sie auf **Erweiterte Einstellungen**.
   - **Status**

     Zeigt an, ob die Einstellungen des SNTP-Servers aktiviert oder deaktiviert sind.
   - **SNTP-Server-Methode**

     Wählen Sie **AUTO** oder **STATISCH**.
     - **AUTO**

       Wenn ein DHCP-Server in Ihrem Netzwerk vorhanden ist, erhält der SNTP-Server seine IP-Adresse automatisch von diesem Server.
     - **STATISCH**

       Geben Sie die gewünschte Adresse ein.
   - **Adresse des primären SNTP-Servers**, **Adresse des sekundären SNTP-Servers**

     Geben Sie die Serveradresse ein (bis zu 64 Zeichen).
   - **Port des primären SNTP-Servers**, **Port des sekundären SNTP-Servers**

     Geben Sie die Portnummer ein (1 bis 65535).

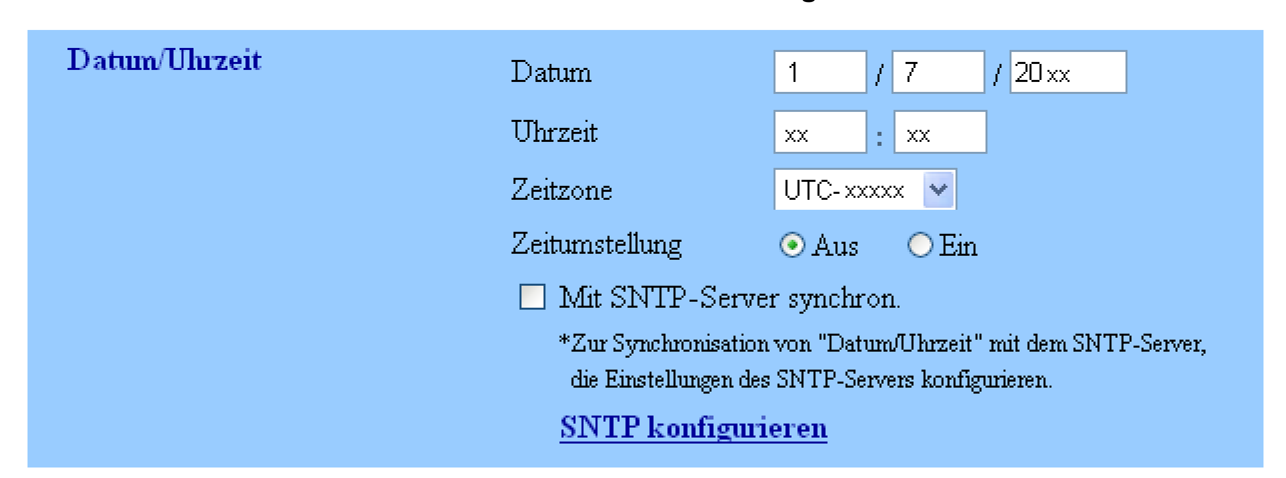
- **Synchronisationsintervall**

  Geben Sie das Intervall, in dem das Gerät mit dem Server synchronisiert werden soll, in Stunden an (1 bis 168 Stunden).



Hinweis

- Sie müssen **Datum/Uhrzeit** konfigurieren, um die Zeit, die vom Gerät verwendet wird, mit der Zeit des SNTP-Zeitservers zu synchronisieren. Klicken Sie auf **Datum/Uhrzeit konfigurieren** und konfigurieren Sie dann **Datum/Uhrzeit** auf dem Bildschirm **Grundeinstellungen**.



- Aktivieren Sie das Kontrollkästchen **Mit SNTP-Server synchron.**. Überprüfen Sie auch Ihre Zeitzonen-Einstellungen. Wählen Sie die Zeitdifferenz zwischen Ihrem Standort und der UTC-Zeit in der Pulldown-Liste **Zeitzone** aus. Die Zeitzone für die USA und Kanada (Eastern Time) ist zum Beispiel UTC-05:00.

- **Synchronisationsstatus**

  Sie können den letzten Synchronisationsstatus überprüfen.

4. Klicken Sie auf **Senden**, um die ausgewählten Einstellungen zu übernehmen.

Druckprotokoll im Netzwerk speichern

Die Funktion „Druckprotokoll im Netzwerk speichern“ ermöglicht das Speichern der Druckprotokoll-Datei Ihres Brother-Gerätes auf einem Netzwerkserver unter Verwendung von CIFS [1]. Sie können die ID, die Art des Druckauftrages, den Auftragsnamen, den Benutzernamen, Datum, Uhrzeit und die Anzahl der gedruckten und farbigen Seiten [2] für jeden Druckauftrag aufzeichnen.

[1] Das CIFS-Protokoll (Common Internet File System) wird unter TCP/IP verwendet und ermöglicht Computern in einem Netzwerk die Freigabe von Dateien in einem Intranet oder im Internet.

[2] Nur für Modelle, die diese Funktion unterstützen.

Die folgenden Druckfunktionen werden im Druckprotokoll aufgezeichnet:

- Druckaufträge von Ihrem Computer
- USB-Direktdruck



Hinweis

- Die Funktion „Druckprotokoll im Netzwerk speichern“ unterstützt die Authentifizierung mit **Kerberos** und **NTLMv2**.

  Zur Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone korrekt einstellen.
- Sie können zum Speichern einer Datei auf dem Server als Dateityp **Text** oder **CSV** wählen.

Einstellungen der Funktion “Druckprotokoll im Netzwerk speichern” mit dem Web Based Management (Webbrowser) konfigurieren

1. Klicken Sie auf der Webseite Ihres Gerätes auf **Administratoreinstellungen** und dann auf **Druckprotok. im Netzw. speichern**.
2. Wählen Sie **Ein** für **Druckprotokoll**.
3. Sie können die folgenden Einstellungen über einen Webbrowser konfigurieren.
   - **Host-Adresse**

     Die Host-Adresse ist der Hostname des CIFS-Servers. Geben Sie die Host-Adresse ein (zum Beispiel: example.com) (bis zu 64 Zeichen) oder die IP-Adresse (zum Beispiel: 192.168.56.189).
   - **Zielordner**

     Geben Sie den Zielordner an, in dem das Protokoll auf dem CIFS-Server gespeichert werden soll (zum Beispiel: brother\abc) (bis zu 60 Zeichen).
   - **Dateiname**

     Geben Sie den gewünschten Dateinamen für das Druckprotokoll ein (bis zu 15 Zeichen).
   - **Dateityp**

     Wählen Sie als Dateityp für das Druckprotokoll **Text** oder **CSV**.

- **Authentifizierungsmethode**

  Wählen Sie die für den Zugang zum CIFS-Server erforderliche Authentifizierungsmethode: **Auto**, **Kerberos** [1] oder **NTLMv2** [2].

  [1] Kerberos ist ein Authentifizierungsprotokoll, das es Geräten oder einzelnen Nutzern ermöglicht, sich an Netzwerk-Servern über eine einmalige Anmeldung (Single Sign-on) sicher auszuweisen.

  [2] NTLMv2 ist die von Windows verwendete Standard-Authentifizierungsmethode zur Anmeldung an Servern.

  Für die Authentifizierung mit Kerberos und NTLMv2 müssen Sie auch die Einstellungen für Datum/Uhrzeit oder das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren.

  Sie können Datum/Uhrzeit und die SNTP-Einstellungen über das Web Based Management konfigurieren.

  - **Auto**: Wenn Sie Auto wählen, sucht das Gerät zunächst nach einem Kerberos-Server. Wenn der Kerberos-Server nicht gefunden wird, wird NTLMv2 als Authentifizierungsmethode verwendet.
  - **Kerberos**: Wählen Sie Kerberos, wenn die Authentifizierung ausschließlich mit Kerberos erfolgen soll.
  - **NTLMv2**: Wählen Sie NTLMv2, wenn die Authentifizierung ausschließlich mit NTLMv2 erfolgen soll.

- **Benutzername**

  Geben Sie einen Benutzernamen für die Authentifizierung ein (bis zu 96 Zeichen).



Hinweis

Wenn der Benutzername Bestandteil einer Domäne ist, geben Sie den Benutzernamen in einem der folgenden Formate ein: user@domain oder domain\user.

- **Kennwort**

  Geben Sie das Kennwort für die Authentifizierung ein (bis zu 32 Zeichen).

- **Kerberos-Serveradresse** (falls erforderlich)

  Geben Sie die KDC-Host-Adresse ein (zum Beispiel: example.com) (bis zu 64 Zeichen) oder die IP-Adresse (zum Beispiel: 192.168.56.189).

4. Unter **Verbindungsstatus** können Sie den letzten Protokollstatus überprüfen. Weitere Informationen finden Sie unter *Fehlermeldungen* auf Seite 49.

5. Klicken Sie auf **Senden**, um Ihre Einstellungen zu übernehmen.

Fehlererkennungseinstellung

Sie können wählen, welche Aktion ausgeführt werden soll, wenn das Druckprotokoll aufgrund eines Netzwerkfehlers nicht auf dem Server gespeichert werden kann.

1. Wählen Sie **Druck abbrechen** oder **Prot.ignorieren&Druck** als **Fehlererkennungseinstellung** unter **Druckprotok. im Netzw. speichern**.

   - **Druck abbrechen**

     Wenn Sie **Druck abbrechen** wählen, werden die Druckaufträge abgebrochen, falls das Druckprotokoll nicht auf dem Server gespeichert werden kann.

   - **Prot.ignorieren&Druck**

     Wenn Sie **Prot.ignorieren&Druck** wählen, druckt das Gerät das Dokument aus, auch wenn das Druckprotokoll nicht auf dem Server gespeichert werden kann.

     Wenn die Funktion zum Speichern des Druckprotokolls wieder zur Verfügung steht, wird das Druckprotokoll wie folgt aufgezeichnet:

     • Wenn das Protokoll nach Beendigung des Ausdruckes nicht gespeichert werden kann, wird das Druckprotokoll ohne die Anzahl der gedruckten und farbigen Seiten aufgezeichnet. (1)

     • Wenn das Druckprotokoll zu Beginn und nach Beendigung des Ausdruckes nicht gespeichert werden kann, wird kein Druckprotokoll dieses Auftrags aufgezeichnet. Wenn die Funktion wieder zur Verfügung steht, wird im Protokoll angezeigt, dass ein Fehler aufgetreten ist. (2)

     Beispiel eines Druckprotokolls:

```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1,Print (Network), "Doc01.doc","user01", 25/01/2009, 14:21:32, 10,10
2,Print (Network), "Doc02.doc","user01", 25/01/2009, 14:45:30, ?, ?     (1)
3,Print(USB), "Report01.els", "Mike", 25/01/2009, 15:20:30, 13, 10
4,<ERROR>, ?, ?, ?, ?, ?, ?                                             (2)
5,Print (Network), "Doc03.doc","user01", 25/01/2009, 16:12:50, 40, 10
```

2. Klicken Sie auf **Senden**, um Ihre Einstellungen zu übernehmen.

6

Fehlermeldungen

Sie können den Fehlerstatus im Display Ihres Gerätes oder den **Verbindungsstatus** im Web Based Management überprüfen.

- `Server-Zeitlimit`

  Diese Meldung wird angezeigt, wenn keine Verbindung zum Server hergestellt werden kann.
  Stellen Sie Folgendes sicher:

  - Ihre Serveradresse ist korrekt.
  - Ihr Server ist an das Netzwerk angeschlossen.
  - Das Gerät ist an das Netzwerk angeschlossen.

- `Authentifizierungsfehler`

  Diese Meldung wird angezeigt, wenn Ihre **Authentifizierungseinstellung** nicht richtig ist.
  Stellen Sie Folgendes sicher:

  - Benutzername [1] und Kennwort sind in der Authentifizierungseinstellung richtig eingegeben.

    [1] Wenn der Benutzername Bestandteil einer Domäne ist, geben Sie den Benutzernamen in einem der folgenden Formate ein: user@domain oder domain\user.

  - Vergewissern Sie sich, dass die Zeit des Protokolldateien-Servers mit der Zeit des SNTP-Servers bzw. den Einstellungen von **Datum/Uhrzeit** übereinstimmt.
  - Stellen Sie sicher, dass die SNTP-Zeitserver-Einstellungen richtig konfiguriert sind, so dass die dort eingestellte Zeit mit der zur Authentifizierung verwendeten Zeit von Kerberos bzw. NTLMv2 übereinstimmt. Wenn kein SNTP-Server verwendet wird, vergewissern Sie sich, dass die Einstellungen für **Datum/Uhrzeit** und **Zeitzone** mit dem Web Based Management richtig konfiguriert wurden, so dass die Zeit, die das Gerät verwendet, mit der Zeit des Servers übereinstimmt, der die Authentifizierung bereitstellt.

- `Dateizugriffsfehler`

  Diese Meldung wird angezeigt, wenn nicht auf den Zielordner zugegriffen werden kann.
  Stellen Sie Folgendes sicher:

  - Der Verzeichnisname ist richtig.
  - In das Verzeichnis kann geschrieben werden.
  - Die Datei ist nicht gesperrt.

- `Datum/Uhrzeit falsch`

  Diese Meldung wird angezeigt, wenn Ihr Gerät keine Zeitinformationen vom SNTP-Zeitserver erhält.
  Stellen Sie Folgendes sicher:

  - Vergewissern Sie sich mit dem Web Based Management, dass die Einstellungen zum Zugriff auf die SNTP-Zeit korrekt sind.
  - Wenn kein SNTP-Server verwendet wird, vergewissern Sie sich, dass die oder das Web Based Management vorgenommenen Einstellungen für Datum und Uhrzeit mit der Zeit des Servers übereinstimmen, der die Authentifizierung bereitstellt.



Hinweis

Wenn Sie die Option **Druck abbrechen** im Web Based Management gewählt haben, wird die Meldung `Fehl:ZugriffProt` ca. 30 Sekunden lang im Display angezeigt.

Funktion „Druckprotokoll im Netzwerk speichern“ zusammen mit Benutzersperre 2.0 verwenden

Wenn die Benutzersperre 2.0 aktiviert ist, werden die Namen der registrierten Nutzer für die Funktionen und USB-Direktdruck von der Funktion “Druckprotokoll im Netzwerk speichern” aufgezeichnet.

Beispiel eines Druckprotokolls mit Benutzern der Benutzersperre 2.0:

```
Id, Type, Job Name, User Name, date, Time, Print Pages, Color Pages
1, Copy, -, -, 29/4/2009, 9:36:06, 1,1
2, Fax, -, -, 29/4/2009, 22:38:30, 1,0
3, Copy, -, Bob, 30/4/2009, 9:06:17, 1,0
4, Fax, -, Bob, 30/4/2009, 9:02:13, 2,0
5, USB Direct, -, John, 30/4/2009, 10:58:52, 1,1
```

6

7 Sicherheitsfunktionen

Übersicht

Heutzutage sind Netzwerke und die Daten, die darin übertragen werden, vielen Sicherheitsrisiken ausgesetzt. Ihr Brother-Gerät verwendet moderne Protokolle zur Netzwerksicherheit und Datenverschlüsselung. Diese Netzwerkfunktionen können in Ihr Gesamtsicherheitskonzept eingegbunden werden, um Ihre Daten zu schützen und den Zugriff von unberechtigten Personen auf Ihr Gerät zu verhindern. In diesem Kapitel wird erklärt, wie diese Funktionen konfiguriert werden können.

Sie können die folgenden Sicherheitsfunktionen konfigurieren:

- Netzwerkgerät mit SSL/TLS sicher verwalten (Siehe *Netzwerkgerät mit SSL/TLS sicher verwalten* auf Seite 52.)
- Netzwerkgerät mit dem SNMPv3-Protokoll sicher verwalten (Siehe *Sichere Verwaltung mit dem Web Based Management (Webbrowser)* auf Seite 52 oder *Sichere Verwaltung mit BRAdmin Professional 3 (für Windows®)* auf Seite 61.)
- Sicherer Druck von Dokumenten mit SSL/TLS (Siehe *Sicherer Druck von Dokumenten mit SSL/TLS* auf Seite 54.)
- E-Mails sicher senden und empfangen (Siehe *E-Mails sicher senden oder empfangen* auf Seite 55.)
- IEEE 802.1x-Authentifizierung verwenden (Siehe *IEEE 802.1x-Authentifizierung verwenden* auf Seite 58.)
- Sichere Verwaltung mit BRAdmin Professional 3 (für Windows®) (Siehe *Sichere Verwaltung mit BRAdmin Professional 3 (für Windows®)* auf Seite 61.)
- Zertifikate für die sichere Verwaltung (Siehe *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.)
- Mehrerer Zertifikate verwalten (Siehe *Mehrere Zertifikate verwalten* auf Seite 72.)

Hinweis

Wir empfehlen, das Telnet-, FTP- und das TFTP-Protokoll zu deaktivieren. Der Zugriff auf das Gerät mit diesen Protokollen ist nicht sicher. (Informationen zur Konfiguration der Protokolleinstellungen finden Sie unter *Geräteeinstellungen mit dem Web Based Management (Webbrowser) konfigurieren* auf Seite 40.)

Netzwerkgerät mit SSL/TLS sicher verwalten

Um die Sicherheit Ihres Netzwerkgerätes zu gewährleisten, müssen Sie die Verwaltungsprogramme zusammen mit den Sicherheitsprotokollen verwenden.

Sichere Verwaltung mit dem Web Based Management (Webbrowser)

Wir empfehlen, das HTTPS-Protokoll und das SNMPv3-Protokoll zur sicheren Verwaltung zu verwenden. Zur Verwendung des HTTPS-Protokolls sind die folgenden Geräteeinstellungen notwendig.

- Im Gerät müssen ein privates Zertifikat oder ein Zertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wurde, und ein privater Schlüssel (Private Key) installiert sein. (Zur Installation eines Zertifikates und eines privaten Schlüssels (Private Key) lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.)
- Das HTTPS-Protokoll muss aktiviert sein. Zur Aktivierung des HTTPS-Protokolls wählen Sie ein installiertes Zertifikat in der Pulldown-Liste der Seite **HTTP-Servereinstellungen** des **Web Based Management** auf der Seite **Protokoll konfigurieren** und aktivieren Sie dann **SSL-Verbindung wird verwendet (Port 443)**. (Nähere Informationen zum Zugriff auf die Seite **Protokoll konfigurieren** finden Sie unter *Geräteeinstellungen mit dem Web Based Management (Webbrowser) konfigurieren* auf Seite 40.)

7

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „`https://Common Name/`“ ein. (Wobei „`Common Name`“ der allgemeine Name ist, den Sie dem Zertifikat zugewiesen haben, zum Beispiel eine IP-Adresse. Wie Sie dem Zertifikat einen allgemeinen Namen zuweisen können, lesen Sie unter *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.)
   - Zum Beispiel:

     `https://192.168.1.2/` (wenn der allgemeine Name die IP-Adresse des Druckers ist)
3. Nun können Sie mit HTTPS auf das Gerät zugreifen.
   Wir empfehlen, die sichere Verwaltung (SNMPv3) zusammen mit dem HTTPS-Protokoll zu verwenden. Zur Verwendung des SNMPv3-Protokolls gehen Sie wie unten beschrieben vor.

Hinweis

Sie können die SNMP-Einstellungen auch mit BRAdmin Professional 3 oder Web BRAdmin ändern.

4. Klicken Sie auf **Netzwerkkonfiguration**.
5. Geben Sie einen Benutzernamen und ein Kennwort ein. Der Standardbenutzername ist „**admin**“ und das Standard-Kennwort ist „**access**“.
6. Klicken Sie auf **Protokoll konfigurieren**.

7 Vergewissern Sie sich, dass die **SNMP**-Einstellung aktiviert ist, und klicken Sie dann auf **Erweitere Einstellungen** von **SNMP**.

8 Nun können Sie die SNMP-Einstellungen im unten gezeigten Bildschirm vornehmen.



Es stehen drei Betriebsarten für den SNMP-Modus zur Auswahl.

■ **SNMPv3 Lese-/Schreibzugriff**

In diesem Modus verwendet der PrintServer die Version 3 des SNMP-Protokolls. Wenn Sie den PrintServer sicher verwalten möchten, sollten Sie diesen Modus verwenden.



Hinweis

Wenn Sie die Einstellung **SNMPv3 Lese-/Schreibzugriff** verwenden, beachten Sie bitte Folgendes:

- Der PrintServer kann nur mit BRAdmin Professional 3, Web BRAdmin oder mit dem Web Based Management verwaltet werden.
- Wir empfehlen, eine sichere SSL-Verbindung (HTTPS) zu verwenden.
- Mit Ausnahme von BRAdmin Professional 3 und Web BRAdmin werden alle Anwendungen, die SNMPv1/v2c verwenden, eingeschränkt. Um die Verwendung von SNMPv1/v2c-Anwendungen zuzulassen, aktivieren Sie die Betriebsart **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff** oder **SNMPv1/v2c Lese-/Schreibzugriff**.

- **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff**

  In diesem Modus verwendet der PrintServer den Lese-/Schreibzugriff der Version 3 und den Nur-Lesezugriff der Version 1 und Version 2c des SNMP-Protokolls.



Wenn Sie den Modus **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff** verwenden, arbeiten einige Brother-Anwendungen, die auf den PrintServer zugreifen (z. B. BRAdmin Light), nicht richtig, da sie lediglich den Nur-Lesezugriff der Version 1 und der Version 2c erlauben. Wenn Sie alle Anwendungen verwenden möchten, stellen Sie den **SNMPv1/v2c-Lese-/Schreibzugriff** ein.

- **SNMPv1/v2c Lese-/Schreibzugriff**

  In diesem Modus verwendet der PrintServer Version 1 und Version 2c des SNMP-Protokolls. Sie können in diesem Modus alle Brother-Anwendungen verwenden. Beachten Sie jedoch, dass dieser Modus nicht sicher ist, da er keine Benutzerauthentifizierung verwendet und die Daten nicht verschlüsselt werden.



Weitere Informationen finden Sie in der Hilfe des Web Based Managements.

Sicherer Druck von Dokumenten mit SSL/TLS

Zum sicheren Druck von Dokumenten über das Internet können Sie das IPPS-Protokoll verwenden.



- Die Kommunikation über IPPS kann den unbefugten Zugriff auf den PrintServer nicht verhindern.
- IPPS steht für Windows® 2000/XP, Windows Vista®, Windows® 7 und Windows Server® 2003/2008 zur Verfügung.

Zur Verwendung des IPPS-Protokolls sind die folgenden Geräteeinstellungen notwendig.

- Im Gerät müssen ein privates Zertifikat oder ein Zertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wurde, und ein privater Schlüssel (Private Key) installiert sein. Zur Installation eines Zertifikates und eines privaten Schlüssels (Private Key) lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.
- Das IPPS-Protokoll muss aktiviert sein. Zur Aktivierung des IPPS-Protokolls wählen Sie ein installiertes Zertifikat in der Pulldown-Liste der Seite **HTTP-Servereinstellungen** von **IPP** auf der Seite **Protokoll konfigurieren** und aktivieren Sie dann **SSL-Verbindung wird verwendet (Port 443)**. Nähere Informationen zum Zugriff auf die Seite **Protokoll konfigurieren** finden Sie unter *Geräteeinstellungen mit dem Web Based Management (Webbrowser) konfigurieren* auf Seite 40.

E-Mails sicher senden oder empfangen

Konfiguration mit dem Web Based Management (Webbrowser)

Sie können das sichere Senden von E-Mails mit Benutzerauthentifizierung oder das Senden und Empfangen von E-Mails mit SSL/TLS im Web Based Management konfigurieren.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „`http://printer’s IP address/`“ ein (wobei „`printer’s IP address`“ für die IP-Adresse des Druckers steht).
   - Zum Beispiel:

     `http://192.168.1.2/`
3. Klicken Sie auf **Netzwerkkonfiguration**.
4. Geben Sie einen Benutzernamen und ein Kennwort ein. Der Standardbenutzername ist „**admin**“ und das Standard-Kennwort ist „**access**“.
5. Klicken Sie auf **Protokoll konfigurieren**.
6. Klicken Sie auf **Erweiterte Einstellung** von **POP3/SMTP** und vergewissern Sie sich, dass der Status von **POP3/SMTP** auf **Aktivieren** steht.
7. Auf dieser Seite können Sie die **POP3/SMTP**-Einstellungen konfigurieren.

Hinweis

- Weitere Informationen finden Sie in der Hilfe des Web Based Managements.
- Durch das Senden einer Test-E-Mail können Sie die Konfiguration der E-Mail-Einstellungen überprüfen.

8. Klicken Sie nach der Konfiguration auf **Senden**. Nun erscheint das Dialogfeld zum Testes des E-Mail-Empfangs/Versands.
9. Folgen Sie den Anweisungen auf dem Bildschirm, wenn Sie Ihre aktuellen Einstellungen prüfen möchten.

E-Mail mit Benutzerauthentifizierung senden

Dieses Gerät unterstützt die Methoden POP vor SMTP und SMTP-AUTH zum Senden einer E-Mail über einen E-Mail-Server, der eine Benutzerauthentifizierung erfordert. Diese Methoden verhindern den unbefugten Zugriff auf den E-Mail-Server. Sie können diese Einstellungen mit dem Web Based Management, BRAdmin Professional 3 oder Web BRAdmin konfigurieren. Sie können die Authentifizierungsmethoden POP vor SMTP und SMTP-AUTH für die E-Mail-Benachrichtigung und für E-Mail-Berichte verwenden.

E-Mail-Server Einstellungen

Die Einstellungen für die SMTP-Authentifizierung müssen mit der Methode, die der E-Mail-Server verwendet, übereinstimmen. Sprechen Sie die Konfiguration des E-Mail-Servers mit Ihrem Netzwerkadministrator oder Internetanbieter ab.

Für eine SMTP-Serverauthentifizierung muss auch **SMTP-AUTH** als **Authentifizierungsmethode für SMTP-Server** aktiviert sein.

SMTP-Einstellungen

- Sie können die SMTP-Portnummer mit dem Web Based Management ändern. Dies ist besonders dann hilfreich, wenn Ihr Internetanbieter den OP25B-Dienst zur Blockierung von Port 25 (“Outbound Port 25 Blocking“) implementiert hat.
- Durch Ändern der SMTP-Portnummer in eine bestimmte Portnummer, die Ihr Internetanbieter für den SMTP-Server verwendet (zum Beispiel Port 587), können Sie dann über den SMTP-Server E-Mails versenden.
- Wenn Sie sowohl POP vor SMTP als auch SMTP-AUTH verwenden können, empfehlen wir SMTP-AUTH.
- Wenn Sie als Authentifizierungsmethode für SMTP-Server POP vor SMTP wählen, müssen Sie die POP3-Einstellungen konfigurieren. Sie können auch die APOP-Methode verwenden.

E-Mails mit SSL/TLS sicher senden oder empfangen

Dieses Gerät unterstützt SSL/TLS zum Senden und Empfangen von E-Mails über einen E-Mail-Server, der eine sichere SSL/TLS-Kommunikation erfordert. Um E-Mails über einen E-Mail-Server, der die SSL/TLS-Kommunikation verwendet, zu senden oder zu empfangen, müssen SMTP über SSL/TLS oder POP3 über SSL/TLS richtig konfiguriert sein.

Server-Zertifikat verifizieren

- Wenn Sie SSL oder TLS für **SMTP über SSL/TLS** oder **POP3 über SSL/TLS** gewählt haben, wird das Kontrollkästchen **Server-Zertifikat verifizieren** automatisch aktiviert, um das Server-Zertifikat zu überprüfen.
  - Bevor Sie das Server-Zertifikat überprüfen, müssen Sie das CA-Zertifikat importieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat. Wenden Sie sich bei Fragen zu CA-Zertifikaten an Ihren Systemadministrator. Zum Import des Zertifikates lesen Sie *CA-Zertifikate importieren und exportieren* auf Seite 72.
  - Wenn Sie das Server-Zertifikat nicht überprüfen müssen, deaktivieren Sie **Server-Zertifikat verifizieren**.

Portnummer

- Wenn Sie SSL oder TLS wählen, werden die Einstellungen des **SMTP-Port** oder **POP3-Port** an das Protokoll angepasst. Wenn Sie die Portnummer manuell ändern möchten, geben Sie die Portnummer ein, nachdem Sie **SMTP über SSL/TLS** oder **POP3 über SSL/TLS** gewählt haben.
- Sie müssen die Kommunikationsmethoden POP3/SMTP konfigurieren, um Sie an den E-Mail-Server anzupassen. Für ausführliche Informationen zu den Einstellungen des E-Mail-Servers wenden Sie sich an Ihren Netzwerkadministrator oder Internetservice-Anbieter.

  In den meisten Fällen erfordern die sicheren Webmail-Dienste die folgenden Einstellungen:

  (SMTP)

  SMTP Port: 587

  Authentifizierungsmethode für SMTP-Server: SMTP-AUTH

  SMTP über SSL/TLS: TLS

  (POP3)

  POP3 Port: 995

  POP3 über SSL/TLS: SSL

IEEE 802.1x-Authentifizierung verwenden

Sie können die IEEE 802.1x-Authentifizierung für ein verkabeltes Netzwerk oder ein Wireless-Netzwerk konfigurieren.

Um die IEEE 802.1x-Authentifizierung zu verwenden, müssen Sie ein Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, installieren. Fragen Sie Ihren Netzwerkadministrator oder Internetanbieter, ob der Import eines CA-Zertifikates erforderlich ist. (Zur Installation eines Zertifikates lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.)

IEEE 802.1x-Authentifizierung mit dem Web Based Management (Webbrowser) konfigurieren

Wenn Sie die IEEE 802.1x-Authentifizierung für verkabelte Netzwerke oder Wireless-Netzwerke mit dem Web Based Management konfigurieren, gehen Sie wie folgt vor.

Sie können zur Konfiguration der IEEE 802.1x-Authentifizierung auch die folgende Software verwenden:

(Verkabeltes Netzwerk)

- BRAdmin Professional 3

(Wireless-Netzwerk)

- Wireless Setup-Assistent über das Funktionstastenfeld (Weitere Informationen finden Sie unter *Gerät für ein Wireless-Firmennetzwerk konfigurieren* auf Seite 20.)
- Wireless Setup-Assistenten auf der CD-ROM (Weitere Informationen finden Sie unter *Wireless-Konfiguration mit dem Brother-Installationsprogramm (für HL-4570CDW(T))* auf Seite 26.)
- BRAdmin Professional 3

7

Hinweis

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, das Zertifikat, das Sie verwenden möchten, zu notieren. Zur Installation des Zertifikates lesen Sie *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.
- Bevor Sie das Server-Zertifikat überprüfen, müssen Sie das CA-Zertifikat importieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat. Wenden Sie sich bei Fragen zu CA-Zertifikaten an Ihren Systemadministrator. Zum Import des Zertifikates lesen Sie *CA-Zertifikate importieren und exportieren* auf Seite 72.
- Ausführliche Informationen zu den einzelnen Zertifikaten siehe *Zertifikate für Gerätesicherheit verwenden* auf Seite 62.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „`http://machine's IP address/`“ ein (wobei „`machine's IP address`“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     `http://192.168.1.2/`



Hinweis

- Falls Sie ein Domänen-Namensystem (DNS) verwenden oder die Verwendung von NetBIOS-Namen aktiviert haben, können Sie einen anderen Namen wie zum Beispiel „Shared_Printer“ anstelle der IP-Adresse eingeben.
  - Zum Beispiel:

  `http://Shared_Printer/`

  Wenn Sie die Verwendung von NetBIOS-Namen aktiviert haben, können Sie auch den Knotennamen verwenden.
  - Zum Beispiel:

  `http://brnxxxxxxxxxxxx/`

  Den NetBIOS-Namen können Sie der Netzwerk-Konfigurationsliste entnehmen. (Zum Ausdrucken der Netzwerk-Konfigurationsliste lesen Sie *Netzwerk-Konfigurationsliste drucken* auf Seite 35.)
- Macintosh-Nutzer können einfach durch Klicken auf das Gerätesymbol im **Status Monitor**-Bildschirm auf das Web Based Management zugreifen. Weitere Informationen finden Sie im *Benutzerhandbuch*.

3. Klicken Sie auf **Netzwerkkonfiguration**.
4. Geben Sie einen Benutzernamen und ein Kennwort ein. Der Standardbenutzername ist „**admin**“ und das Standardkennwort ist „**access**“.
5. (Verkabelt) Klicken Sie auf **802.1x (verkabelt) konfigurieren**.
   (Wireless) Klicken Sie auf **Wireless-Einstellungen konfigurieren** und auf die Registerkarte **Firmenbereich**.
6. Sie können nun die Einstellungen zur IEEE 802.1x-Authentifizierung konfigurieren.
   - Wenn Sie die IEEE 802.1x-Authentifizierung für ein verkabeltes Netzwerk aktivieren möchten, markieren Sie **Aktivieren** für **802.1x-Status (verkabelt)** auf der Seite **802.1x (verkabelt) konfigurieren**.
   - Ausführliche Informationen zur IEEE 802.1x-Authentifizierung und den inneren Authentifizierungsmethoden finden Sie im Handbuch *Netzwerkbegriffe*.
   - Wenn Sie die EAP-TLS-Authentifizierung verwenden, müssen Sie das CA-Zertifikat das zur Verifizierung installiert wurde (gezeigt mit dem Zertifikatsnamen), in der Pulldown-Liste **Client-Zertifikat** auswählen.
   - Wenn Sie die Authentifizierung mit EAP-FAST, PEAP, EAP-TTLS oder EAP-TLS gewählt haben, können Sie die Verifizierungsmethode in der Pulldown-Liste **Server-Zertifikat-Verifizierung** wählen. Sie können das Server-Zertifikat mit Hilfe des zuvor importierten CA-Zertifikates verifizieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat.

   Sie können die folgenden Verifizierungsmethoden in der Pulldown-Liste **Server-Zertifikat-Verifizierung** wählen.
   - **Keine Verifizierung**

     Das Server-Zertifikat ist immer vertrauenswürdig. Die Verifizierung wird nicht ausgeführt.

- **CA-Zert.**

  Die Verifizierungsmethode zur Überprüfung der CA-Zuverlässigkeit des Server-Zertifikates mit Hilfe des CA-Zertifikates, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat.

- **CA-Zert. + Server-ID**

  Die Verifizierungsmethode zur Überprüfung des allgemeinen Namens [1] des Server-Zertifikates, zusätzlich zur Überprüfung der CA-Zuverlässigkeit des Server-Zertifikates.

[1] Die Überprüfung des allgemeinen Namens vergleicht den allgemeinen Namen des Server-Zertifikates mit der als **Server-ID** konfigurierten Zeichenkette. Bevor Sie diese Methode verwenden, fragen Sie Ihren Systemadministrator nach dem allgemeinen Namen des Server-Zertifikates und konfigurieren Sie dann die **Server-ID**.

7. Klicken Sie nach der Konfiguration auf **Senden**.
(Verkabelt)
Schließen Sie das Gerät nach Abschluss der Konfiguration an das IEEE 802.1x-Netzwerk an. Drucken Sie nach einigen Minuten die Netzwerk-Konfigurationsliste aus, um den **<Wired IEEE 802.1x> Status.** zu überprüfen. (Siehe *Netzwerk-Konfigurationsliste drucken* auf Seite 35 für Informationen zum Drucken der Netzwerk-Konfigurationsliste Ihres PrintServers.)

- **Success**

  Die IEEE 802.1x-Funktion (verkabelt) ist aktiviert und die Authentifizierung war erfolgreich.

- **Failed**

  Die IEEE 802.1x-Funktion (verkabelt) ist aktiviert, die Authentifizierung ist jedoch fehlgeschlagen.

- **Off**

  Die IEEE 802.1x-Funktion (verkabelt) ist nicht verfügbar.

(Wireless)
Kurz nach der Konfiguration wird automatisch ein WLAN-Bericht ausgedruckt. Prüfen Sie die Wireless-Konfiguration im Bericht. Siehe *WLAN-Bericht drucken (für HL-4570CDW(T))* auf Seite 36.

Sichere Verwaltung mit BRAdmin Professional 3 (für Windows®)

Beachten Sie die folgenden Punkte zur sicheren Verwendung von BRAdmin Professional

- Wir empfehlen dringend, stets mit der neuesten Version von BRAdmin Professional 3 bzw. Web BRAdmin zu arbeiten, die Sie von http://solutions.brother.com/ herunterladen können. Bei Verwendung älterer Versionen von BRAdmin [1] zur Verwaltung Ihrer Brother-Geräte ist die Benutzerauthentifizierung nicht sicher.
- Wenn Sie den Zugriff auf Ihr Gerät von älteren BRAdmin-Versionen [1] unterbinden möchten, müssen Sie über das Web Based Management den Zugang von älteren BRAdmin-Versionen [1] über **Erweiterte Einstellung** von **SNMP** auf der Seite **Protokoll konfigurieren** deaktivieren. (Siehe *Sichere Verwaltung mit dem Web Based Management (Webbrowser)* auf Seite 52.)
- Falls Sie sowohl BRAdmin Professional 3 als auch das Web Based Management benutzen, sollten Sie das Web Based Management zusammen mit dem HTTPS-Protokoll verwenden. (Siehe *Sichere Verwaltung mit dem Web Based Management (Webbrowser)* auf Seite 52.)
- Falls Sie mit BRAdmin Professional 3 verschiedene ältere PrintServer [2] zusammen mit neuen PrintServern verwalten, empfehlen wir, für jede Gruppe ein anderes Kennwort zu verwenden. Dadurch wird die Sicherheit der neuen PrintServer sichergestellt.

[1] BRAdmin Professional älter als Version 2.80, Web BRAdmin älter als Version 1.40, BRAdmin Light für Macintosh älter als Version 1.10

[2] NC-2000-Serie, NC-2100p, NC-3100h, NC-3100s, NC-4100h, NC-5100h, NC-5200h, NC-6100h, NC-6200h, NC-6300h, NC-6400h, NC-8000, NC-100h, NC-110h, NC-120w, NC-130h, NC-140w, NC-8100h, NC-9100h, NC-7100w, NC-7200w, NC-2200w

Zertifikate für Gerätesicherheit verwenden

Ihr Brother-Gerät unterstützt verschiedene Sicherheitszertifikate, um eine sichere Verwaltung, Authenzifizierung und Kommunikation mit dem Gerät zu ermöglichen. Die folgenden Sicherheitsfunktionen können mit dem Gerät verwendet werden.

- SSL/TLS-Kommunikation
- IEEE 802.1x-Authentifizierung
- SSL-Kommunikation für SMTP/POP3

Das Brother-Gerät unterstützt die folgenden Zertifikate.

- Privates Zertifikat

  Dieser PrintServer stellt sein eigenes Zertifikat aus. Mit diesem Zertifikat können Sie problemlos die SSL/TLS-Kommunikation nutzen, ohne ein Zertifikat von einer Zertifizierungsstelle zu haben. (Siehe *Zertifikat erstellen und installieren* auf Seite 64.)

- Zertifikat einer Zertifizierungsstelle (CA)

  Es stehen zwei Verfahren zur Verfügung, mit denen ein Zertifikat von einer Zertifizierungsstelle installiert werden kann. Wenn Sie bereits eine Zertifizierungsstelle haben oder ein Zertifikat von einer vertrauten externen Zertifizierungsstelle verwenden möchten:

  - Installation mit einer Zertifikatsignieranforderung (CSR; Certificate Signing Request) von diesem PrintServer. (Siehe *Zertifikatsignieranforderung (CSR) erstellen* auf Seite 69.)
  - Installation mit Import eines Zertifikates und eines privaten Schlüssels (Private Key). (Siehe *Zertifikat und privaten Schlüssel (Private Key) importieren und exportieren* auf Seite 71.)

- CA-Zertifikat

  Wenn Sie ein CA-Zertifikat verwenden, das die Zertifizierungsstelle (CA - Certificate Authority) selbst identifiziert und einen eigenen privaten Schlüssel (Private Key) hat, müssen Sie vor der Konfiguration ein CA-Zertifikat von der Zertifizierungsstelle importieren. (Siehe *CA-Zertifikate importieren und exportieren* auf Seite 72.)



Hinweis

- Wenn Sie die SSL/TLS-Kommunikation verwenden möchten, sollten Sie sich zuerst an Ihren Systemadministrator wenden.
- Wenn Sie den PrintServer auf die werkseitigen Standardeinstellungen zurücksetzen, wird das installierte Zertifikat einschließlich des privaten Schlüssels (Private Key) gelöscht. Wenn Sie nach dem Zurücksetzen des PrintServers dasselbe Zertifikat und denselben privaten Schlüssel (Private Key) verwenden möchten, sollten Sie diese vor dem Zurücksetzen exportieren und danach erneut installieren. (Siehe *Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel exportieren* auf Seite 71.)

Zertifikate mit dem Web Based Management konfigurieren

Diese Funktion kann nur über das Web Based Management konfiguriert werden. Gehen Sie wie folgt vor, um über das Web Based Management auf die Seite zum Konfigurieren des Zertifikates zu gelangen.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „`http://printer's IP address/`“ ein (wobei „`printer's IP address`“ für die IP-Adresse des Druckers steht).
   - Zum Beispiel:

     `http://192.168.1.2/`
3. Klicken Sie auf **Netzwerkkonfiguration**.
4. Geben Sie einen Benutzernamen und ein Kennwort ein. Der Standardbenutzername ist „**admin**“ und das Standard-Kennwort ist „**access**“.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Zertifikat konfigurieren**.
7. Nun können Sie die Zertifikateinstellungen im unten gezeigten Bildschirm vornehmen.

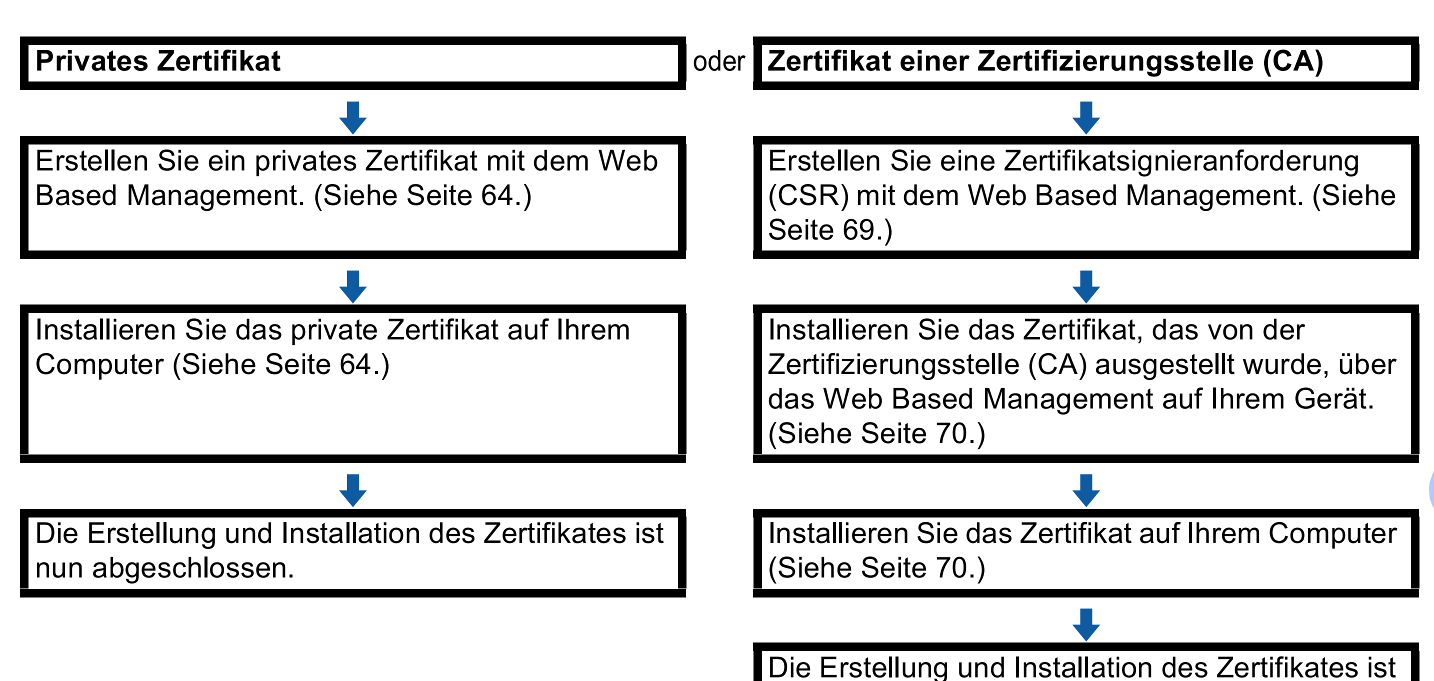



Hinweis

- Funktionen, die grau markiert und nicht verlinkt sind, stehen nicht zur Verfügung.
- Weitere Informationen zur Konfiguration finden Sie in der Hilfe des Web Based Managements.

Zertifikat erstellen und installieren

Schritte zur Erstellung und Installation von Zertifikaten



Privates Zertifikat erstellen und installieren

1. Klicken Sie auf **Privates Zertifikat erstellen** auf der Seite **Zertifikat konfigurieren**.
2. Füllen Sie die Felder **Allgemeine Name** und **Gültigkeitsdauer** aus und klicken Sie dann auf **Senden**.



Hinweis

- In das Feld **Allgemeine Name** müssen weniger als 64 Byte eingegeben werden. Geben Sie eine Kennung ein, zum Beispiel IP-Adresse, Knotenname oder Domänenname, die beim Zugriff auf dieses Gerät über die SSL/TLS-Kommunikation verwendet wird. Standardmäßig wird der Knotenname angezeigt.
- Es erscheint eine Warnung, wenn Sie das IPPS- oder HTTPS-Protokoll verwenden und in die URL einen anderen Namen eingeben, als den der unter **Allgemeine Name** für das Zertifikat benutzt wurde.

3. Das private Zertifikat ist nun erstellt und erfolgreich in Ihrem Gerät gespeichert.
Zur Verwendung der SSL/TLS-Kommunikation muss das private Zertifikat auch auf Ihrem Computer installiert werden. Fahren Sie dazu mit dem nächsten Abschnitt fort.

Privates Zertifikat auf dem Computer installieren

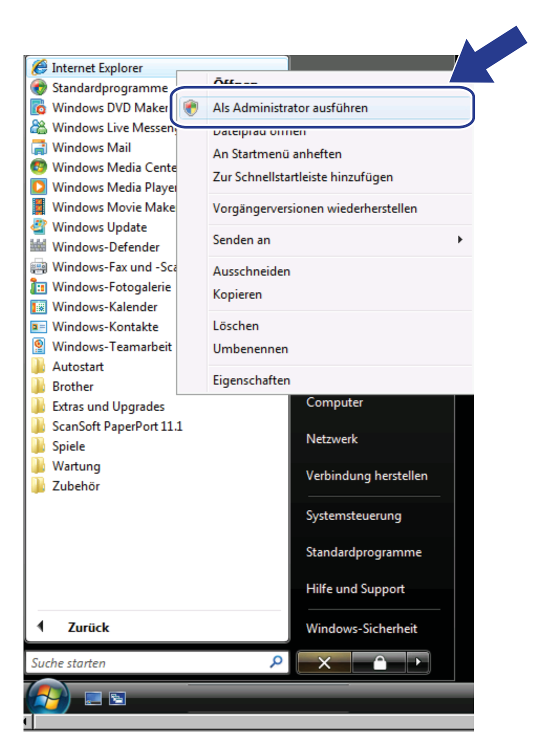


Hinweis

In den folgenden Schritten wird der Microsoft® Internet Explorer® verwenden. Falls Sie einen anderen Webbrowser benutzen, folgen Sie der Anleitung in der Hilfe des Browsers.

Für Nutzer von Windows Vista® und Windows® 7 mit Administratorrechten

1. Klicken Sie auf die Schaltfläche und dann auf **Alle Programme**.
2. Klicken Sie mit der rechten Maustaste auf **Internet Explorer** und klicken Sie dann auf **Als Administrator ausführen**.



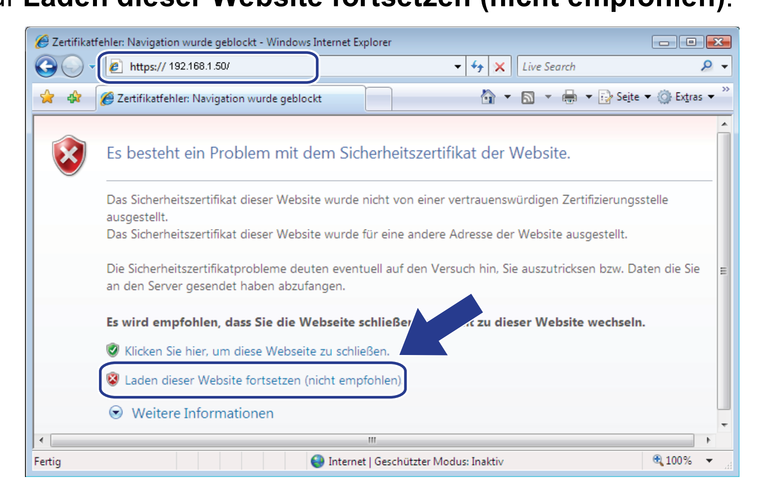


Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird:

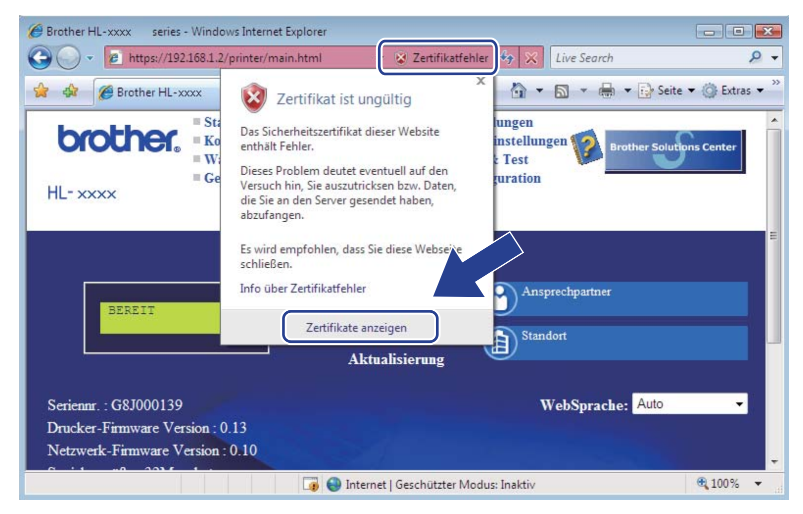
(Windows Vista®) Klicken Sie auf **Fortfahren (Zulassen)**.

(Windows® 7) Klicken Sie auf **Ja**.

3. Geben Sie „`https://printer’s IP address/`“ in Ihren Browser ein, um auf das Gerät zuzugreifen (dabei steht „`printer’s IP address`“ entweder für die IP-Adresse des Druckers oder den Knotennamen, den Sie dem Zertifikat zugewiesen haben.
   Klicken Sie dann auf **Laden dieser Website fortsetzen (nicht empfohlen)**.

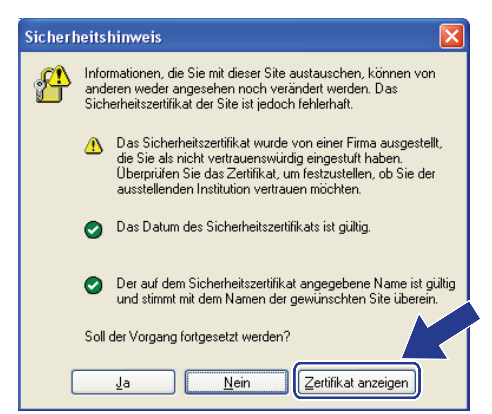


4. Klicken Sie auf **Zertifikatfehler** und dann auf **Zertifikate anzeigen**. Fahren Sie mit Schritt ❹ unter *Für Nutzer von Windows® 2000/XP und Windows Server® 2003/2008* auf Seite 67 fort.

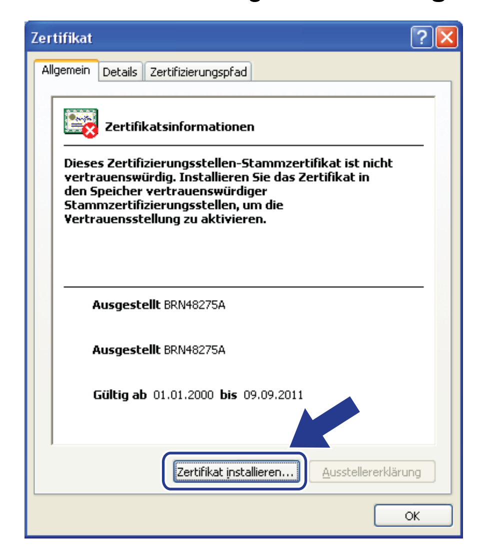


Für Nutzer von Windows® 2000/XP und Windows Server® 2003/2008

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „`https://printer's IP address/`“ in Ihren Browser ein, um auf das Gerät zuzugreifen (dabei steht „`printer's IP address`“ entweder für die IP-Adresse oder den Knotennamen, den Sie dem Zertifikat zugewiesen haben.
3. Wenn das folgende Dialogfeld angezeigt wird, klicken Sie auf **Zertifikat anzeigen**.

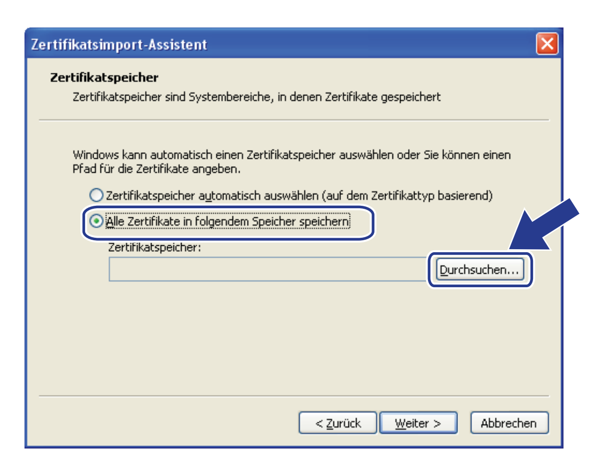


4. Klicken Sie auf **Zertifikat installieren...** in der Registerkarte **Allgemein**.

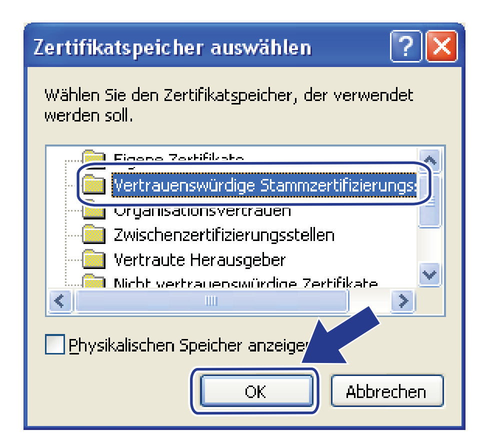


5. Wenn der **Zertifikatsimport-Assistent** erscheint, klicken Sie auf **Weiter**.

6 Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Durchsuchen...**.



7 Wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen** und klicken Sie dann auf **OK**.

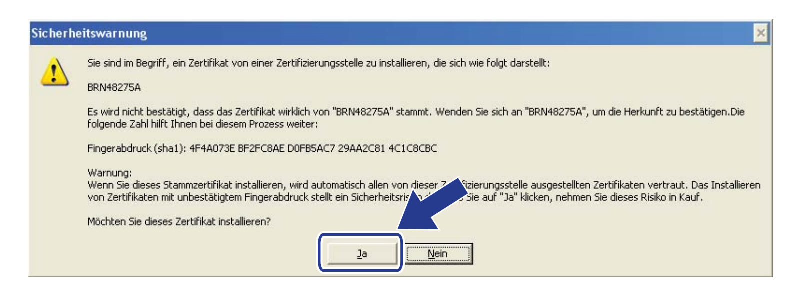


8 Klicken Sie auf **Weiter**.



9 Klicken Sie auf **Beenden**.

10. Klicken Sie auf **Ja**, wenn der Fingerabdruck des Zertifikates korrekt ist.





Hinweis

Den Fingerabdruck (Fingerprint, Thumbprint) finden Sie in der Netzwerk-Konfigurationsliste. (Zum Ausdrucken der Netzwerk-Konfigurationsliste lesen Sie *Netzwerk-Konfigurationsliste drucken* auf Seite 35.)

11. Klicken Sie auf **OK**.

12. Das private Zertifikat ist nun auf Ihrem Computer installiert und die SSL/TLS-Kommunikation ist möglich.

Zertifikatsignieranforderung (CSR) erstellen

1. Klicken Sie auf **Zertifikatsignieranforderung (CSR) erstellen** auf der Seite **Zertifikat konfigurieren**.

2. Füllen Sie das Feld **Allgemeine Name** aus und geben Sie Ihre Informationen, wie die **Organisation** ein. Klicken Sie dann auf **Senden**.

Hinweis

- Es wird empfohlen, das Stammzertifikat von der Zertifizierungsstelle auf Ihrem Computer zu installieren, bevor Sie eine Zertifikatsignieranforderung erstellen.
- In das Feld **Allgemeine Name** müssen weniger als 64 Byte eingegeben werden. Geben Sie eine Kennung ein, zum Beispiel IP-Adresse, Knotenname oder Domänenname, die beim Zugriff auf diesen Drucker über die SSL/TLS-Kommunikation verwendet wird. Standardmäßig wird der Knotenname angezeigt. Der **Allgemeine Name** muss angegeben werden.
- Es erscheint eine Warnung, wenn Sie einen anderen Namen in die URL eingeben, als den allgemeinen Namen, der für das Zertifikat benutzt wurde.
- In die Felder **Organisation**, **Organisationseinheit**, **Ort** und **Bundesland** müssen weniger als 64 Byte eingegeben werden.
- Für **Land** sollte ein Ländercode nach ISO 3166 (2 Zeichen) eingegeben werden.
- Wenn Sie eine X.509v3 -Zertifikaterweiterung konfigurieren, aktivieren Sie das Kontrollkästchen **Erweiterte Partition konfigurieren** und wählen Sie dann **Auto** oder **Manuell**.

3. Wenn der Inhalt der Zertifikatsignieranforderung (CSR) angezeigt wird, klicken Sie auf **Speichern**, um die CSR-Datei auf Ihrem Computer zu speichern.

4. Die Zertifikatsignieranforderung ist nun erstellt.

Hinweis

- Beachten Sie in Bezug auf das Verfahren zum Senden der Zertifikatsignieranforderung an Ihre Zertifizierungsstelle die Richtlinien der Zertifizierungsstelle.
- Wenn Sie die **Stammzertifizierungsstelle des Unternehmens** von Windows Server® 2003/2008 verwenden, empfehlen wir, beim Erstellen des Client-Zertifikates für die sichere Verwaltung den **Webserver** als Zertifikatvorlage zu verwenden. Wenn Sie ein Client-Zertifikat für eine IEEE 802.1x-Umgebung mit EAP-TLS-Authentifizierung erstellen, empfehlen wir, **Benutzer** als Zertifikatvorlage zu verwenden. Weitere Informationen finden Sie auf der SSL-Kommunikationsseite, die Sie über die Hauptseite Ihres Modells unter http://solutions.brother.com/ aufrufen können.

Zertifikat auf dem Gerät installieren

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, installieren Sie es wie folgt auf dem PrintServer.

Hinweis

Es können nur Zertifikate installiert werden, die über die Zertifikatsignieranforderung (CSR) dieses Gerätes ausgestellt wurden. Wenn Sie eine weitere Zertifikatsignieranforderung erstellen möchten, vergewissern Sie sich, das das Zertifikat installiert wurde, bevor Sie eine weitere Zertifikatsignieranforderung erstellen. Erstellen Sie eine weitere Zertifikatsignieranforderung, nachdem Sie das Zertifikat auf dem Gerät installiert haben. Anderenfalls wird die Zertifikatsignieranforderung, die Sie vor der Installation erstellt haben, ungültig.

1. Klicken Sie auf **Zertifikat installieren** auf der Seite **Zertifikat konfigurieren**.

2. Geben Sie die Datei mit dem von einer Zertifizierungsstelle (CA) ausgestellten Zertifikat an und klicken Sie dann auf **Senden**.

3. Das private Zertifikat ist nun erstellt und erfolgreich im Speicher Ihres Gerätes abgelegt.
   Zur Verwendung der SSL/TLS-Kommunikation muss das Stammzertifikat der Zertifizierungsstelle auch auf Ihrem Computer installiert werden. Wenden Sie sich zur Installation an Ihren Netzwerkadministrator.

Zertifikat und privaten Schlüssel (Private Key) importieren und exportieren

Sie können das Zertifikat und den privaten Schlüssel im Gerät speichern und diese durch Import und Export verwalten.

Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel importieren

1. Klicken Sie auf **Zertifikat und Private Key importieren** auf der Seite **Zertifikat konfigurieren**.
2. Geben Sie die Datei an, die Sie importieren möchten.
3. Geben Sie das Kennwort ein, falls die Datei verschlüsselt ist, und klicken Sie dann auf **Senden**.
4. Das Zertifikat und der Private Key wurden nun erfolgreich in Ihr Gerät importiert.
   Zur Verwendung der SSL/TLS-Kommunikation muss auch das Stammzertifikat der Zertifizierungsstelle auf Ihrem Computer installiert werden. Wenden Sie sich zur Installation an Ihren Netzwerkadministrator.

Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel exportieren

1. Klicken Sie auf **Exportieren** neben **Zertifikatliste** auf der Seite **Zertifikat konfigurieren**.
2. Geben Sie das Kennwort ein, wenn Sie die Datei verschlüsseln möchten.

Hinweis

Wenn kein bzw. ein leeres Kennwort verwendet wird, ist die Ausgabe nicht verschlüsselt.

3. Geben Sie das Kennwort zur Bestätigung erneut ein und klicken Sie dann auf **Senden**.
4. Geben Sie an, wo Sie die Datei speichern wollen.
5. Zertifikat und Private Key sind nun erfolgreich zum Computer exportiert worden.

Hinweis

Sie können die exportierte Datei nun importieren.

Mehrere Zertifikate verwalten

Diese Funktion für mehrere Zertifikate erlaubt die Verwaltung von allen installierten Zertifikaten über das Web Based Management. Nach der Installation der Zertifikate können Sie anzeigen lassen, welche Zertifikate über die Seite **Zertifikat konfigurieren** installiert wurden, und dann den Inhalt der einzelnen Zertifikate ansehen, die Zertifikate löschen oder exportieren. Nähere Informationen zum Zugriff auf die Seite **Zertifikat konfigurieren** finden Sie unter *Zertifikate mit dem Web Based Management konfigurieren* auf Seite 63. Das Brother-Gerät ermöglicht das Speichern von bis zu drei privaten Zertifikaten oder bis zu vier Zertifikaten, die von einer Zertifizierungsstelle ausgestellt wurden. Sie können die gespeicherten Zertifikate zur Verwendung des HTTPS/IPPS-Protokolls oder der IEEE 802.1x-Authentifizierung nutzen.

Sie können auch bis zu vier CA-Zertifikate zur Verwendung der IEEE 802.1x-Authentifizierung und von SSL vor SMTP/POP3 speichern.

Wir empfehlen, ein Zertifikat weniger zu speichern und den dritten Speicherplatz für den Fall freizuhalten, dass ein Zertifikat abläuft. Wenn Sie zum Beispiel ein CA-Zertifikat speichern möchten, speichern Sie drei Zertifikate und lassen Sie einen Speicherplatz zur Sicherung frei. Wenn Sie das Zertifikat erneut anfordern, zum Beispiel weil es abgelaufen ist, können Sie ein neues Zertifikat in den freigehaltenen Speicherplatz importieren und erst dann das abgelaufenen Zertifikat löschen, um Konfigurationsfehler zu vermeiden.



Hinweis

Wenn Sie das HTTPS/IPPS-Protokoll oder IEEE 802.1x verwenden, müssen Sie wählen, welches Zertifikat benutzt werden soll.

CA-Zertifikate importieren und exportieren

Sie können ein CA-Zertifikat und einen privaten Schlüssel (Private Key) im Gerät speichern, indem Sie es importieren und exportieren.

CA-Zertifikat und privaten Schlüssel (Private Key) importieren

1. Klicken Sie auf **CA-Zertifikat konfigurieren** auf der Seite **Zertifikat konfigurieren**.
2. Klicken Sie auf **CA-Zertifikat importieren**. Klicken Sie auf **Senden**.

CA-Zertifikat und privaten Schlüssel (Private Key) exportieren

1. Klicken Sie auf **CA-Zertifikat konfigurieren** auf der Seite **Zertifikat konfigurieren**.
2. Wählen Sie das Zertifikat, das Sie exportieren möchten, und klicken Sie auf **Exportieren**. Klicken Sie auf **Senden**.

8 Problemlösung

Übersicht

Dieses Kapitel erklärt, wie Sie Netzwerkprobleme, die bei der Verwendung Ihres Gerätes auftreten können, lösen können. Falls Sie in diesem Kapitel keine Lösung für Ihr Problem finden, besuchen Sie das Brother Solutions Center unter: http://solutions.brother.com/.

Bitte besuchen Sie das Brother Solutions Center unter http://solutions.brother.com/ und klicken Sie auf der Seite für Ihr Modell auf , um die anderen Handbücher herunterzuladen.

Problem identifizieren

Vergewissern Sie sich, dass die folgenden Punkte erfüllt sind, bevor Sie die Problemlösungen lesen.

Prüfen Sie zunächst Folgendes:
Der Netzstecker ist richtig angeschlossen und das Brother-Gerät ist eingeschaltet.
Der Access Point (für wireless), Router oder Hub ist eingeschaltet und die Verbindungsanzeige blinkt.
Alle Transportschutzteile wurden vom Gerät entfernt.
Die Tonerkassetten und die Trommeleinheit sind richtig installiert.
Die vorderen und hinteren Abdeckungen sind ganz geschlossen.
Das Papier ist richtig in die Papierkassette eingelegt.
(Für verkabelte Netzwerke) Ein Netzwerkkabel ist richtig an das Brother-Gerät und den Router oder Hub angeschlossen.

Gehen Sie zur Lösung Ihres Problems zu der in der folgenden Liste angegebenen Seite

- Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen. (Siehe Seite 74.)
- Das Brother-Gerät wird während der Installation des Druckertreibers nicht im Netzwerk gefunden. (Siehe Seite 75.)
- Das Brother-Gerät kann über das Netzwerk nicht drucken. (Siehe Seite 76.)
- Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden. (Siehe Seite 76.)
- Ich verwende Sicherheitssoftware. (Siehe Seite 79.)
- Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten. (Siehe Seite 79.)

Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen.

Frage	Schnittstelle	Lösung
Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?	wireless	■ Überprüfen Sie die Sicherheitseinstellungen und wählen Sie die richtigen Einstellungen. • Der Name des Herstellers bzw. die Modellnummer des WLAN Access Points/Routers werden eventuell als die standardmäßigen Sicherheitseinstellungen verwendet. • Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde, um die Sicherheitseinstellungen herauszufinden. • Wenden Sie sich an den Hersteller Ihres WLAN Access Points/Routers, an Ihren Internetanbieter oder Netzwerkadministrator. ■ Informationen zur SSID und zu Netzwerkschlüsseln finden Sie unter SSID, Netzwerkschlüssel und Kanäle im Handbuch *Netzwerkbegriffe*.
Verwenden Sie eine MAC-Adressenfilterung?	wireless	Überprüfen Sie, ob die MAC-Adresse des Brother-Gerätes im Filter erlaubt ist. Sie können die MAC-Adresse Ihres Brother-Gerätes über das Funktionstastenfeld des Gerätes ermitteln. (Siehe *Funktionstabelle und werkseitige Standardeinstellungen* auf Seite 37.)
Befindet sich Ihr WLAN Access Point/Router im Stealth-Modus? (SSID wird nicht gesendet)	wireless	■ Sie sollten den SSID-Namen oder der Netzwerkschlüssel manuell eingeben. ■ Überprüfen Sie den SSID-Namen bzw. den Netzwerkschlüssel anhand der Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde, und konfigurieren Sie die Wireless-Netzwerkeinstellungen erneut. (Weitere Informationen finden Sie unter *Konfiguration des Gerätes, wenn die SSID nicht rundgesendet wird* auf Seite 17.)
Ich habe alle oben genannten Punkte überprüft und ausgeführt, kann jedoch die Konfiguration des Wireless-Netzwerkes noch immer nicht abschließen. Was kann ich sonst noch tun?	wireless	Verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung. Siehe *Das Brother-Gerät kann über das Netzwerk nicht drucken. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.* auf Seite 76.

Das Brother-Gerät wird während der Installation des Druckertreibers nicht im Netzwerk gefunden.

Frage	Schnittstelle	Lösung
Verwenden Sie Sicherheitssoftware?	verkabelt/ wireless	■ Wählen Sie im Installer-Dialogfeld erneut die Option zur Suche nach dem Brother-Gerät. ■ Erlauben Sie den Zugriff, wenn während der Installation des Druckertreibers eine Warnmeldung der Sicherheitssoftware angezeigt wird. ■ Für weitere Informationen zur Sicherheitssoftware lesen Sie *Ich verwende Sicherheitssoftware.* auf Seite 79.
Ist Ihr Gerät zu weit entfernt vom WLAN Access Point/Router aufgestellt?	wireless	Stellen Sie das Brother-Gerät zur Konfiguration der Wireless-Netzwerkeinstellungen innerhalb eines Abstandes von ca. 1 m vom WLAN Access Point/Router auf.
Befinden sich Hindernisse (zum Beispiel Wände oder Möbel) zwischen Ihrem Gerät und dem WLAN Access Point/Router?	wireless	Stellen Sie das Brother-Gerät so auf, dass der Funkkontakt nicht gestört wird, oder stellen Sie es näher an den WLAN Access Point/Router.
Befindet sich ein Wireless-Computer, ein Gerät, das Bluetooth unterstützt, ein Mikrowellengerät oder ein digitales schnurloses Telefon in der Nähe des Gerätes oder des WLAN Access Points/Routers?	wireless	Stellen Sie alle Geräte in größerer Entfernung vom Brother-Gerät bzw. vom WLAN Access Point/Router auf.

Das Brother-Gerät kann über das Netzwerk nicht drucken.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.

Frage	Schnittstelle	Lösung
Verwenden Sie Sicherheitssoftware?	verkabelt/ wireless	Siehe *Ich verwende Sicherheitssoftware.* auf Seite 79.
Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?	verkabelt/ wireless	■ Überprüfen Sie die IP-Adresse und die Subnetzmaske. Vergewissern Sie sich, dass sowohl die IP-Adresse und die Subnetzmaske des Computers als auch des Brother-Gerätes korrekt zugeordnet wurden und dass sie sich im selben Netzwerk befinden. Weitere Informationen zur Überprüfung der IP-Adresse und Subnetzmaske erhalten Sie bei Ihrem Netzwerkadministrator oder im Brother Solutions Center unter http://solutions.brother.com/. ■ (Windows®) Überprüfen Sie die IP-Adresse und Subnetzmaske mit dem Dienstprogramm zum Reparieren der Netzwerkverbindung. Verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung, um die Netzwerkeinstellungen des Brother-Gerätes zu reparieren. Es weist die korrekte IP-Adresse und Subnetzmaske zu. Zur Verwendung des Dienstprogramms zum Reparieren der Netzwerkverbindung, bitten Sie Ihren Netzwerkadministrator um weitere Informationen und gehen Sie dann wie folgt vor: **Hinweis** • (Windows® 2000 Professional/XP/XP Professional x64 Edition/Windows Vista®/Windows® 7) Sie müssen sich mit Administratorrechten anmelden. • Vergewissern Sie sich, dass das Brother-Gerät eingeschaltet und über das Netzwerk mit Ihrem Computer verbunden ist.

Das Brother-Gerät kann über das Netzwerk nicht drucken.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden. (Fortsetzung)

Frage	Schnittstelle	Lösung
Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen? (Fortsetzung)	verkabelt/ wireless	1 (Windows® 2000/XP, Windows Server® 2003/2008) Klicken Sie auf **Start**, **Alle Programme** (**Programme** für Windows® 2000), **Zubehör** und **Windows Explorer**, und dann **Arbeitsplatz**. (Windows Vista®/Windows® 7) Klicken Sie auf und **Computer**. 2 Doppelklicken Sie auf **Lokaler Datenträger (C:)**, **Programme** oder **Programme (x86)** für Nutzer von 64-Bit-Betriebssystemen, **Browny02**, **Brother**, **BrotherNetTool.exe**, um das Programm auszuführen. **Hinweis** Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird: (Windows Vista®) Klicken Sie auf **Fortfahren**. (Windows® 7) Klicken Sie auf **Ja**. 3 Folgen Sie den Anweisungen auf dem Bildschirm. 4 Überprüfen Sie das Resultat der Diagnose, indem Sie die Netzwerk-Konfigurationsliste ausdrucken. **Hinweis** Das Programm zum Reparieren der Netzwerkverbindung wird automatisch gestartet, wenn Sie das Kontrollkästchen **Programm zum Reparieren der Netzwerkverbindung aktivieren** in der Registerkarte **Optionen** des Status Monitors aktivieren. Dies wird nicht empfohlen, wenn der Netzwerkadministrator die IP-Adresse fest eingestellt hat (Statisch), weil sonst die IP-Adresse automatisch geändert wird. Wenn auch nach der Verwendung des Dienstprogramms zum Reparieren der Netzwerkverbindung die IP-Adresse und Subnetzmaske nicht richtig zugewiesen sind, fragen Sie Ihren Netzwerkadministrator nach diesen Informationen oder besuchen Sie das Brother Solutions Center unter http://solutions.brother.com/.

Das Brother-Gerät kann über das Netzwerk nicht drucken.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden. (Fortsetzung)

Frage	Schnittstelle	Lösung
Konnte Ihr vorheriger Druckauftrag nicht richtig ausgeführt werden?	verkabelt/ wireless	■ Wenn sich der fehlgeschlagene Druckauftrag noch immer in der Druckwarteschlange Ihres Computer befindet, löschen Sie ihn. ■ Doppelklicken Sie auf das Druckersymbol im folgenden Ordner und wählen Sie dann **Alle Druckaufträge abbrechen** im **Drucker**-Menü. (Windows® 2000) **Start**, **Einstellungen** und dann **Drucker**. (Windows® XP) **Start** und **Drucker und Faxgeräte**. (Windows Vista®) , **Systemsteuerung**, **Hardware und Sound** und dann **Drucker**. (Windows® 7) , **Systemsteuerung**, **Geräte und Drucker** und dann **Drucker und Faxgeräte**.
Verbinden Sie das Brother-Gerät drahtlos mit dem Netzwerk?	wireless	■ Drucken Sie den WLAN-Bericht aus, um den Status der Wireless-Verbindung zu prüfen. (Weitere Informationen zum Drucken des Berichtes finden Sie unter *WLAN-Bericht drucken (für HL-4570CDW(T))* auf Seite 36.) Falls im WLAN-Bericht ein Fehlercode ausgedruckt wurde, lesen Sie Problemlösung in der *Installationsanleitung*. ■ Siehe *Das Brother-Gerät wird während der Installation des Druckertreibers nicht im Netzwerk gefunden.* auf Seite 75.
Ich habe alle oben genannten Punkte überprüft und ausgeführt, aber das Brother-Gerät druckt nicht. Was kann ich sonst noch tun?	verkabelt/ wireless	Deinstallieren Sie den Druckertreiber und installieren Sie ihn dann erneut.

Ich verwende Sicherheitssoftware.

Frage	Schnittstelle	Lösung
Haben Sie während der Installation des Druckertreibers dem Starten von Programmen zugestimmt oder beim Verwenden der Druck-Funktionen die Sicherheitswarnung im Dialogfeld akzeptiert?	verkabelt/ wireless	Wenn Sie die Sicherheitswarnung im Dialogfeld nicht akzeptiert haben, verweigert die Firewall-Funktion Ihrer Sicherheitssoftware möglicherweise den Zugriff. Einige Sicherheitsprogramme blockieren eventuell den Zugriff, ohne ein Dialogfeld zur Sicherheitswarnung anzuzeigen. Lesen Sie in der Anleitung der Sicherheitssoftware nach, wie Sie den Zugriff erlauben können, oder fragen Sie den Hersteller.
Ich möchte die notwendigen Portnummern für die Sicherheitssoftware-Einstellungen wissen.	verkabelt/ wireless	Die folgenden Portnummern werden von den Brother-Netzwerkfunktionen verwendet: ■ Drucken im Netzwerk → Portnummer 137 / Protokoll UDP ■ BRAdmin Light → Portnummer 161 / Protokoll UDP Siehe die Anleitung der Sicherheitssoftware oder wenden Sie sich an den Hersteller, um ausführliche Informationen zum Öffnen der Ports zu erhalten.

8

Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten.

Frage	Schnittstelle	Lösung
Ist Ihr Brother-Gerät, Ihr Access Point/Router bzw. Ihr Netzwerk-Hub eingeschaltet?	verkabelt/ wireless	Stellen Sie sicher, dass Sie alle Punkte unter *Prüfen Sie zunächst Folgendes:* auf Seite 73 überprüft haben.
Wo kann ich die Netzwerkeinstellungen des Brother-Gerätes, wie die IP-Adresse, finden?	verkabelt/ wireless	Drucken Sie die Netzwerk-Konfigurationsliste aus. Siehe *Netzwerk-Konfigurationsliste drucken* auf Seite 35.
Wie kann ich den Verbindungsstatus des Brother-Gerätes prüfen?	verkabelt/ wireless	Drucken Sie die Netzwerk-Konfigurationsliste aus und prüfen Sie, ob als **Ethernet Link Status** oder **Wireless Link Status** der Hinweis **Link OK** ausgedruckt wurde. Wenn für **Link Status** der Hinweis **Link Down** oder **Failed to Associate** erscheint, beginnen Sie noch einmal mit *Prüfen Sie zunächst Folgendes:* auf Seite 73.

Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten. (Fortsetzung)

Frage	Schnittstelle	Lösung
Können Sie das Brother-Gerät vom Computer aus mit dem „Ping“-Befehl ansprechen?	verkabelt/ wireless	Verwenden Sie den “Ping”-Befehl mit der IP-Adresse oder dem Knotennamen des Brother-Gerätes von Ihrem Computer aus. ■ Erfolgreich → Ihr Brother-Gerät arbeitet korrekt und ist mit demselben Netzwerk wie Ihr Computer verbunden. ■ Nicht erfolgreich → Ihr Brother-Gerät ist nicht mit demselben Netzwerk wie Ihr Computer verbunden. (Windows®) Wenden Sie sich an Ihren Netzwerkadministrator und verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung, um die IP-Adresse und die Subnetzmaske automatisch zuzuweisen. Für weitere Informationen zum Dienstprogramm zum Reparieren der Netzwerkverbindung lesen Sie *(Windows®) Überprüfen Sie die IP-Adresse und Subnetzmaske mit dem Dienstprogramm zum Reparieren der Netzwerkverbindung.* unter *Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?* auf Seite 76. (Macintosh) Vergewissern Sie sich, dass die IP-Adresse und die Subnetzmaske korrekt eingestellt sind. Siehe *Überprüfen Sie die IP-Adresse und die Subnetzmaske.* unter *Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?* auf Seite 76.
Verbindet sich das Brother-Gerät mit dem Wireless-Netzwerk?	wireless	Drucken Sie den WLAN-Bericht aus, um den Status der Wireless-Verbindung zu prüfen. (Weitere Informationen zum Drucken des Berichtes finden Sie unter *WLAN-Bericht drucken (für HL-4570CDW(T))* auf Seite 36.) Falls im WLAN-Bericht ein Fehlercode ausgedruckt wurde, lesen Sie Problemlösung in der *Installationsanleitung*.
Ich habe alle oben genannten Punkte überprüft und ausgeführt, aber das Problem tritt weiter auf. Was kann ich sonst noch tun?	verkabelt/ wireless	Lesen Sie die Anleitung, die Sie mit Ihrem WLAN Access Point/Router erhalten haben, um die SSID- und Netzwerkschlüssel-Informationen zu ermitteln und sie richtig einzustellen. Für weitere Informationen zur SSID und dem Netzwerkschlüssel lesen Sie *Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?* unter *Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen.* auf Seite 74.

A Anhang A

Unterstützte Protokolle und Sicherheitsfunktionen

Schnittstelle	Ethernet	10/100BASE-TX
	Wireless [1]	IEEE802.11b/g (Infrastruktur-Modus / Ad-hoc-Modus)
Netzwerk (allgemein)	Protokoll (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), WINS/NetBIOS-Namensauflösung, DNS-Resolver, mDNS, LLMNR-Responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP -Server, TELNET-Server, HTTP/HTTPS-Server, TFTP-Client und -Server, SMTP-Client, SNMPv1/v2c/v3, ICMP, LLTD-Responder, Web Services (Drucken), CIFS-Client, SNTP-Client
	Protokoll (IPv6)	NDP, RA, DNS-Resolver, mDNS, LLMNR-Responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP -Server, TELNET-Server, HTTP/HTTPS-Server, TFTP-Client und -Server, SMTP-Client, SNMPv1/v2c/v3, ICMPv6, LLTD-Responder, Web Services (Drucken), CIFS-Client, SNTP-Client
Netzwerk (Sicherheit)	Verkabelt	APOP, POP vor SMTP, SMTP-AUTH, SSL/TLS (IPPS, HTTPS, SMTP, POP), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Wireless [1]	WEP 64/128 Bit, WPA-PSK (TKIP/AES), WPA2-PSK (AES), APOP, POP vor SMTP, SMTP-AUTH, SSL/TLS (IPPS, HTTPS, SMTP, POP), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
Netzwerk (Wireless) [1]	Wireless-Zertifizierung	Wi-Fi Certification Mark Lizenz, Wi-Fi Protected Setup (WPS) Identifier Mark Lizenz, AOSS-Logo

[1] Für HL-4570CDW(T)

B Stichwortverzeichnis

A

B

E

F

G

H

I

M

N

P

R

S

T

V

W

Z



Netzwerkbegriffe

In diesem Netzwerkbegriffe-Handbuch finden Sie grundlegende Informationen zu den erweiterten Netzwerkfunktionen von Brother-Geräten sowie zu allgemeinen Netzwerkbegriffen und anderen gebräuchlichen Terminologien.

Die unterstützten Protokolle und Netzwerkfunktionen können sich je nach verwendetem Modell unterscheiden. Um herauszufinden, welche Funktionen und Netzwerkprotokolle unterstützt werden, lesen Sie das *Netzwerkhandbuch*. Das neueste Handbuch können Sie vom Brother Solutions Center unter http://solutions.brother.com/ herunterladen.

Sie können auch die neusten Treiber und Dienstprogramme für Ihr Gerät herunterladen, Antworten auf häufig gestellte Fragen (FAQs) und Tipps zur Problemlösung finden oder sich über besondere Lösungen rund um das Drucken informieren.



Version 0

GER

Definition der Hinweise

In diesem Handbuch wird das folgende Symbol verwendet:

Hinweis	Hinweise informieren Sie, wie auf eine bestimmte Situation reagiert werden sollte, oder geben Ihnen hilfreiche Tipps zur beschriebenen Funktion.

WICHTIGER HINWEIS

- Dieses Produkt entspricht den Bestimmungen des Landes, für das es zugelassen wurde. Verwenden Sie dieses Produkt daher nur in dem Land, in dem Sie es gekauft haben, da es in anderen Ländern eventuell gegen die Telekommunikationsbestimmungen und Anschlussvorschriften verstößt.
- Windows® XP steht in diesem Dokument für Windows® XP Professional, Windows® XP Professional x64 Edition und Windows® XP Home Edition.
- Windows Server® 2003 steht in diesem Dokument für Windows Server® 2003 und Windows Server® 2003 x64 Edition.
- Windows Server® 2008 steht in diesem Dokument für Windows Server® 2008 und Windows Server® 2008 R2.
- Windows Vista® steht in diesem Handbuch für alle Ausgaben von Windows Vista®.
- Windows® 7 steht in diesem Handbuch für alle Ausgaben von Windows® 7.
- Bitte besuchen Sie das Brother Solutions Center unter http://solutions.brother.com/ und klicken Sie auf der Seite für Ihr Modell auf Handbücher, um die anderen Handbücher herunterzuladen.

Inhaltsverzeichnis

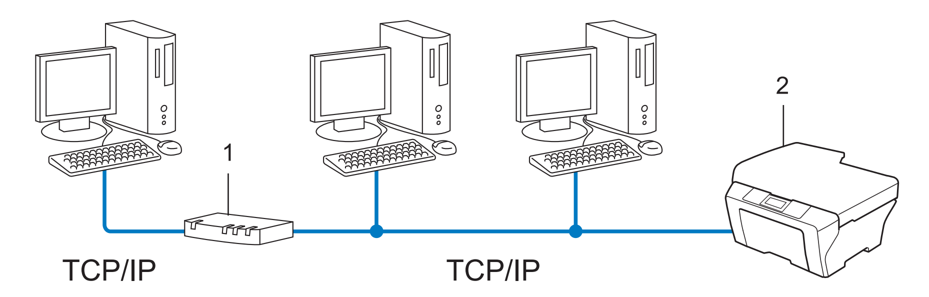
1 Arten der Netzwerkverbindungen und Protokolle

Arten der Netzwerkverbindungen

Beispiel einer verkabelten Netzwerkverbindung

Peer-to-Peer-Druck über TCP

In einer Peer-to-Peer-Umgebung sendet jeder Computer Daten direkt an jedes Gerät und empfängt von diesen Geräten auch Daten. Dateizugriffe und gemeinsam genutzte Geräte werden nicht über einen zentralen Server gesteuert.



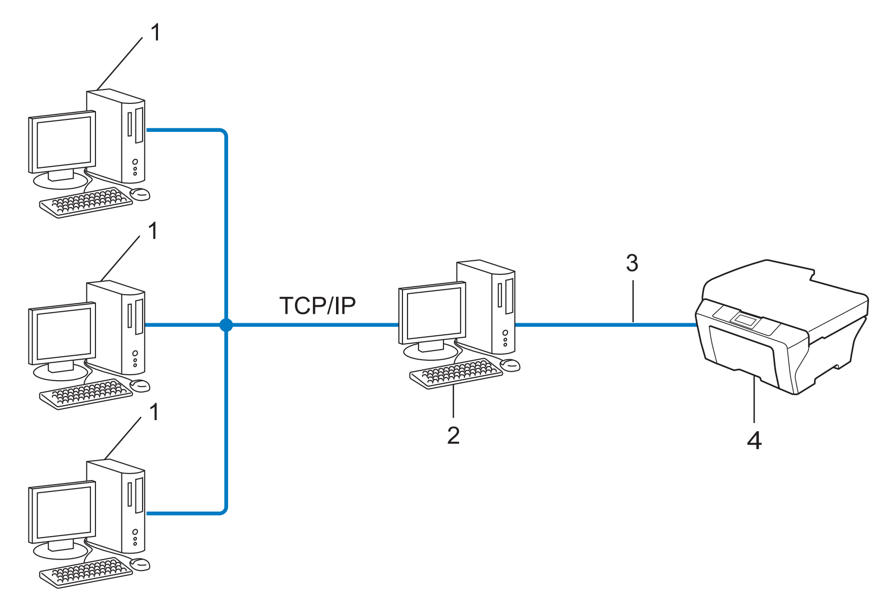
1 Router

2 Netzwerkgerät (Ihr Gerät)

- Für kleinere Netzwerke mit 2 oder 3 Computern empfehlen wir das Drucken in einer Peer-to-Peer-Umgebung, da sie einfacher zu konfigurieren ist als das Drucken über das gemeinsame Netzwerk. Siehe *Drucken über das gemeinsame Netzwerk* auf Seite 2.
- Jeder Computer muss das TCP/IP-Protokoll verwenden.
- Die IP-Adresse des Brother-Gerätes muss entsprechend konfiguriert werden.
- Wenn Sie einen Router verwenden, muss die Gateway-Adresse der verwendeten Computer und des Brother-Gerätes konfiguriert werden.

Drucken über das gemeinsame Netzwerk

In einer Netzwerkumgebung sendet jeder Computer Daten über einen zentral verwalteten Computer. Dieser Computer wird in der Regel „Server“ oder „Druckserver“ genannt. Seine Aufgabe ist es, das Drucken aller Druckaufträge zu steuern.



1 Client-Computer

2 „Server“ oder „Druckserver“

3 TCP/IP, USB oder Parallel (soweit verfügbar)

4 Netzwerkgerät (Ihr Gerät)

- In größeren Netzwerken empfehlen wir das Einrichten von Netzwerkdruckern.
- Der „Server“ bzw. „Druckserver“ muss das TCP/IP-Protokoll verwenden.
- Falls das Brother-Gerät nicht über die USB- oder Parallelschnittstelle an den Server angeschlossen wurde, muss dem Gerät eine entsprechende IP-Adresse zugewiesen werden.

Protokolle

TCP/IP-Protokolle und ihre Funktionen

Protokolle sind standardisierte Regeln zur Datenübertragung in einem Netzwerk. Durch Protokolle erhalten Nutzer Zugang zu den Netzwerk-Ressourcen.

Der mit diesem Brother-Gerät verwendete PrintServer unterstützt das TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol).

Das TCP/IP-Protokoll ist das am häufigsten verwendete Protokoll für die Kommunikation, wie zum Beispiel im Internet und per E-Mail. Dieses Protokoll kann unter fast allen Betriebssystemen verwendet werden, wie Windows®, Windows Server®, Mac OS X und Linux®. Die folgenden TCP/IP-Protokolle sind für dieses Brother-Gerät verfügbar.



Hinweis

- Sie können die Protokolleinstellungen über die HTTP-Schnittstelle (Webbrowser) konfigurieren. (Siehe das *Netzwerkhandbuch*.)
- Um herauszufinden, welche Protokolle Ihr Brother-Gerät unterstützt, lesen Sie das *Netzwerkhandbuch*.
- Informationen zu den unterstützten Sicherheitsprotokollen finden Sie unter *Sicherheitsprotokolle* auf Seite 19.

DHCP/BOOTP/RARP

Über die Protokolle DHCP/BOOTP/RARP kann die IP-Adresse automatisch konfiguriert werden.



Hinweis

Um die Protokolle DHCP/BOOTP/RARP zu verwenden, wenden Sie sich bitte an Ihren Netzwerkadministrator.

APIPA

Wenn Sie die IP-Adresse nicht manuell (über das Funktionstastenfeld des Gerätes (nur Modelle mit Display) oder mit Hilfe der BRAdmin-Software) oder automatisch (mit einem DHCP/BOOTP/RARP-Server) zuweisen, vergibt das APIPA-Protokoll (Automatic Private IP Addressing) automatisch eine im Bereich von 169.254.1.0 bis 169.254.254.255 liegende IP-Adresse.

ARP

ARP (Address Resolution Protocol) übernimmt in einem TCP/IP-Netzwerk die Zuordnung einer IP-Adresse zu einer MAC-Adresse.

DNS-Client

Der Brother PrintServer unterstützt die DNS-Client-Funktion (DNS: Domain Name System). Dadurch kann der PrintServer mit anderen Geräten Daten austauschen, indem er sie mit ihrem DNS-Namen anspricht.

NetBIOS-Namensauflösung

Die NetBIOS-Namensauflösung (Network Basic Input/Output System) ermöglicht es, während einer bestehenden Netzwerkverbindung die IP-Adresse des anderen Gerätes über die Verwendung seines NetBIOS-Namens zu erhalten.

WINS

WINS (Windows Internet Name Service) ist ein Dienst, der Informationen für die NetBIOS-Namensauflösung liefert, indem er eine IP-Adresse einem NetBIOS-Namen des lokalen Netzwerkes zuordnet.

LPR/LPD

Häufig verwendete Druckprotokolle innerhalb eines TCP/IP-Netzwerkes.

SMTP-Client

Ein SMTP-Client (Simple Mail Transfer Protocol) wird zum Versenden von E-Mails über das Internet oder Intranet verwendet.

Custom Raw Port (Standardeinstellung ist Port 9100)

Ein weiteres häufig verwendetes Druckprotokoll innerhalb von TCP/IP-Netzwerken. Es ermöglicht die interaktive Datenübertragung.

IPP

Mit dem Internet Printing Protocol (IPP Version 1.0) können Dokumente über das Internet direkt auf jedem erreichbaren Gerät ausgedruckt werden.

 **Hinweis**

Näheres zum IPPS-Protokoll finden Sie unter *Sicherheitsprotokolle* auf Seite 19.

mDNS

Mit mDNS kann sich der Brother PrintServer automatisch für den Betrieb in einer Mac OS® X-Umgebung mit einfacher Netzwerkkonfiguration konfigurieren.

TELNET

Mit dem TELNET-Protokoll können Sie die entfernten Netzwerkgeräte in einem TCP/IP-Netzwerk von Ihrem Computer aus steuern.

SNMP

Das SNMP-Protokoll (Simple Network Management Protocol) wird für die Verwaltung von Netzwerkgeräten verwendet, wie z. B. Computer, Router und netzwerkfähige Brother-Geräte. Der Brother PrintServer unterstützt SNMPv1, SNMPv2c und SNMPv3.



Hinweis

Näheres zum SNMPv3-Protokoll finden Sie unter *Sicherheitsprotokolle* auf Seite 19.

LLMNR

Das LLMNR-Protokoll (Link-Local Multicast Name Resolution) löst die Namen benachbarter Computer auf, falls im Netzwerk kein DNS-Server (Domain Name System) vorhanden ist. Die LLMNR-Responder-Funktion arbeitet in einer IPv4- und IPv6-Umgebung, wenn ein Computer mit LLMNR-Sender-Funktion, z. B. mit Windows Vista® und Windows® 7, verwendet wird.

Web Services

Mit dem Web Services-Protokoll kann unter Windows Vista® oder Windows® 7 der Brother-Druckertreiber mit einem Rechtsklick auf das Gerätesymbol im Ordner **Netzwerk** installiert werden. (Siehe *Installation für das Drucken im Netzwerk mit Web Services (Windows Vista® und Windows® 7)* auf Seite 15.) Mit Web Services können Sie auch von Ihrem Computer aus den aktuellen Status Ihres Gerätes prüfen.

HTTP

Das HTTP-Protokoll wird zur Übermittlung von Daten zwischen einem Webserver und einem Webbrowser verwendet.



Hinweis

Näheres zum HTTPS-Protokoll finden Sie unter *Sicherheitsprotokolle* auf Seite 19.

FTP (für die Scan-to-FTP-Funktion)

Das FTP-Protokoll (File Transfer Protocol) ermöglicht es dem Brother-Gerät, gescannte Schwarzweiß- oder Farbdokumente direkt an einen FTP-Server zu senden, der entweder lokal an Ihrem Netzwerk oder an das Internet angeschlossen ist.

SNTP

Das SNTP-Protokoll (Simple Network Time Protocol) wird zur Synchronisation der Systemzeit von Computern in einem TCP/IP-Netzwerk verwendet. Sie können die SNTP-Einstellungen über das Web Based Management (Webbrowser) konfigurieren. (Weitere Informationen finden Sie im *Netzwerkhandbuch*.)

CIFS

CIFS (Common Internet File System) ist das Standardverfahren, das Computernutzer zur gemeinsamen Verwendung von Dateien und Druckern unter Windows® verwenden.

LDAP

Das LDAP-Protokoll (Lightweight Directory Access Protocol) ermöglicht es dem Brother-Gerät, nach Informationen wie Faxnummern und E-Mail-Adressen auf einem LDAP-Server zu suchen.

IPv6

IPv6 ist die neue Generation von Internetprotokollen. Weitere Informationen zum IPv6-Protokoll finden Sie auf der Website für Ihr Gerät unter http://solutions.brother.com/.

Sonstige Protokolle

LLTD

Mit Hilfe des LLTD-Protokolls (LLTD: Link Layer Topology Discovery) können Sie das Brother-Gerät ganz einfach in der **Netzwerkübersicht** von Windows Vista®/Windows® 7 finden. Ihr Brother-Gerät wird mit einem speziellen Symbol und dem Knotennamen angezeigt. Standardmäßig ist dieses Protokoll deaktiviert. Sie können LLTD mit dem Web Based Management (Webbrowser) (siehe das *Netzwerkhandbuch*) und dem Dienstprogramm BRAdmin Professional 3 aktivieren. Besuchen Sie die Download-Seite für Ihr Modell unter http://solutions.brother.com/, um BRAdmin Professional 3 herunterzuladen.

2 Gerät für ein Netzwerk konfigurieren

IP-Adressen, Subnetzmasken und Gateways

Um ein Gerät in einer vernetzten TCP/IP-Umgebung zu verwenden, müssen Sie die IP-Adresse und Subnetzmaske konfigurieren. Die dem PrintServer zugewiesene IP-Adresse muss zum selben logischen Netzwerk gehören wie Ihre Hostcomputer. Ist dies nicht der Fall, müssen Sie die Subnetzmaske und Gateway-Adresse richtig konfigurieren.

IP-Adresse

Eine IP-Adresse ist eine Zahlenfolge, die jedes mit dem Netzwerk verbundene Gerät identifiziert. Eine IP-Adresse besteht aus vier Zahlen, die durch Punkte voneinander getrennt sind. Jede Zahl liegt im Bereich von 0 bis 255.

- Beispiel: In einem kleinen Netzwerk werden in der Regel die letzten Zahlen geändert.
  - `192.168.1.1`
  - `192.168.1.2`
  - `192.168.1.3`

Wie dem PrintServer die IP-Adresse zugeordnet wird:

Wenn ein DHCP/BOOTP/RARP-Server in Ihrem Netzwerk vorhanden ist, erhält der PrintServer seine IP-Adresse automatisch von diesem Server.



Hinweis

In kleineren Netzwerken kann auch der Router als DHCP-Server dienen.

Weitere Informationen zu DHCP, BOOTP und RARP finden Sie unter
IP-Adresse mit DHCP konfigurieren auf Seite 21.
IP-Adresse mit BOOTP konfigurieren auf Seite 23.
IP-Adresse mit RARP konfigurieren auf Seite 22.

Wenn Sie keinen DHCP/BOOTP/RARP-Server verwenden, weist das APIPA-Protokoll (Automatic Private IP Addressing) automatisch eine IP-Adresse zwischen 169.254.1.0 und 169.254.254.255 zu. Weitere Informationen zu APIPA finden Sie unter *IP-Adresse mit APIPA konfigurieren* auf Seite 23.

Subnetzmaske

Eine Subnetzmaske schränkt die Netzwerkkommunikation ein.

- Beispiel: Computer 1 kann Daten mit Computer 2 austauschen
  - Computer 1

    IP-Adresse: 192.168. 1. 2

    Subnetzmaske: 255.255.255.000
  - Computer 2

    IP-Adresse: 192.168. 1. 3

    Subnetzmaske: 255.255.255.000

0 in der Subnetzmaske bedeutet, dass bei diesem Teil der Adresse die Kommunikation nicht eingeschränkt ist. Im Beispiel oben kann daher mit jedem Gerät kommuniziert werden, das eine IP-Adresse hat, die mit 192.168.1.x beginnt (wobei x. für eine Zahl zwischen 0 und 255 steht.)

Gateway (und Router)

Ein Gateway ist eine Einrichtung im Netzwerk, die als Zugang zu einem anderen Netzwerk dient und über das Netzwerk übertragene Daten an einen bestimmten Ort übermittelt. Der Router weiß, wohin die Daten geleitet werden müssen, die am Gateway eintreffen. Falls sich ein Zielort in einem externen Netzwerk befindet, überträgt der Router die Daten zum externen Netzwerk. Wenn Ihr Netzwerk mit anderen Netzwerken kommuniziert, müssen Sie eventuell die Gateway-IP-Adresse konfigurieren. Falls Sie die Gateway-IP-Adresse nicht kennen, wenden Sie sich an Ihren Netzwerkadministrator.

IEEE 802.1x-Authentifizierung

IEEE 802.1x ist ein IEEE-Standard für verkabelte und Wireless-Netzwerke, der den Zugriff von nicht autorisierten Netzwerkgeräten beschränkt. Ihr Brother-Gerät (Bittsteller) sendet über Ihren Access Point (Authentifizierer) eine Authentifizierungsanforderung an einen RADIUS-Server (Authentifizierungsserver). Nachdem die Anforderung durch den RADIUS-Server verifiziert, d. h. überprüft und bestätigt wurde, kann Ihr Gerät auf das Netzwerk zugreifen.

Authentifizierungsmethoden

- LEAP (für ein Wireless-Netzwerk)

  Das Cisco LEAP-Protokoll (Light Extensible Authentication Protocol) wurde von Cisco Systems Inc. entwickelt und verwendet zur Authentifizierung eine Benutzer-ID sowie ein Kennwort.

- EAP-FAST

  Das EAP-FAST-Protokoll (Extensible Authentication Protocol - Flexible Authentication via Secured Tunnel) wurde von Cisco Systems Inc. entwickelt. Es verwendet zur Authentifizierung eine Benutzer-ID sowie ein Kennwort und symmetrische Schlüsselalgorithmen zur Authentifizierung über einen Tunnel.

  Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungen:

  - EAP-FAST/NONE
  - EAP-FAST/MS-CHAPv2
  - EAP-FAST/GTC

- EAP-MD5 (für ein verkabeltes Netzwerk)

  EAP-MD5 (Extensible Authentication Protocol-Message Digest algorithm 5) verwendet eine Benutzer-ID und ein Kennwort für eine Challenge-Response-Authentifizierung (Anfrage-Antwort-Authentifizierung).

- PEAP

  PEAP (Protected Extensible Authentication Protocol) wurde von Microsoft Corporation, Cisco Systems und RSA Security entwickelt. PEAP erzeugt zum Senden einer Benutzer-ID und eines Kennwortes einen verschlüsselten SSL/TLS-Tunnel (Secure Sockets Layer/Transport Layer Security) zwischen einem Client und einem Authentifizierungsserver. PEAP ermöglicht eine gegenseitige Authentifizierung von Server und Client.

  Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungen:

  - PEAP/MS-CHAPv2
  - PEAP/GTC

- EAP-TTLS

  EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) wurde von Funk Software und Certicom entwickelt. EAP-TTLS erzeugt zwischen einem Client und einem Authentifizierungsserver einen ähnlichen verschlüsselten SSL-Tunnel zum Senden einer Benutzer-ID und eines Kennwortes wie PEAP. EAP-TTLS ermöglicht eine gegenseitige Authentifizierung von Server und Client.

  Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungen:

  - EAP-TTLS/CHAP
  - EAP-TTLS/MS-CHAP
  - EAP-TTLS/MS-CHAPv2
  - EAP-TTLS/PAP

- EAP-TLS

  EAP-TLS (Extensible Authentication Protocol Transport Layer Security) erfordert eine Authentifizierung über ein digitales Zertifikat sowohl beim Client als auch beim Authentifizierungsserver.

3 Wireless-Netzwerk: Konzepte und Terminologien

Netzwerk festlegen

SSID (Service Set Identifier) und Kanäle

Sie müssen den SSID-Namen und einen Kanal konfigurieren, um das Wireless-Netzwerk, zu dem eine Verbindung hergestellt werden soll, festzulegen.

- SSID

  Jedes Wireless-Netzwerk hat einen eigenen, eindeutigen Netzwerknamen, die sogenannte SSID oder ESSID (Extended Service Set Identifier). Die SSID ist ein bis zu 32 Byte großer Wert, der dem Access Point zugewiesen wird. Wireless-Netzwerkgeräte, die Sie dem Wireless-Netzwerk zuordnen möchten, müssen dem Access Point entsprechend eingestellt sein. Der Access Point und die Wireless-Netzwerkgeräte senden in regelmäßigen Abständen Wireless-Datenpakete (sogenannte Beacons), welche die SSID-Informationen enthalten. Wenn Ihr Wireless-Netzwerkgerät ein Beacon empfängt, kann darüber festgestellt werden, welches Wireless-Netzwerk nahe genug ist, damit seine Funkwellen Ihr Gerät erreichen.

- Kanäle

  Wireless-Netzwerke verwenden Kanäle. Jeder Wireless-Kanal liegt auf einer anderen Frequenz. In einem Wireless-Netzwerk können bis zu 14 verschiedene Kanäle genutzt werden. Allerdings ist die Anzahl der verfügbaren Kanäle in vielen Ländern beschränkt.

Sicherheitsbegriffe

Authentifizierung und Verschlüsselung

In den meisten Wireless-Netzwerken werden Sicherheitseinstellungen verwendet. Diese Sicherheitseinstellungen legen die Art der Authentifizierung (wie sich das Gerät im Netzwerk anmeldet) und die Art der Verschlüsselung (wie die Daten zum Versenden im Netzwerk verschlüsselt werden) fest. **Wenn Sie diese Einstellungen bei der Konfiguration Ihres Brother Wireless-Gerätes nicht richtig vornehmen, kann sich das Gerät nicht mit dem Wireless-Netzwerk verbinden.** Gehen Sie deshalb besonders sorgfältig vor, wenn Sie diese Einstellungen konfigurieren. Im *Netzwerkhandbuch* finden Sie Informationen dazu, welche Authentifizierungs- und Verschlüsselungsmethoden Ihr Brother Wireless-Gerät unterstützt.

Authentifizierungs- und Verschlüsselungsmethoden für private Wireless-Netzwerke

Ein privates Wireless-Netzwerk ist ein kleines Netzwerk, zum Beispiel wenn Sie Ihr Gerät in einem Wireless-Netzwerk zu Hause (ohne IEEE 802.1x-Unterstützung) verwenden.

Wenn Sie Ihr Gerät in einem Wireless-Netzwerk mit IEEE 802.1x-Unterstützung verwenden möchten, lesen Sie *Authentifizierungs- und Verschlüsselungsmethoden für Wireless-Netzwerke in Firmen und Unternehmen* auf Seite 13.

Authentifizierungsmethoden

- Open system (offenes System)

  Wireless-Geräte können ohne Authentifizierung auf das Netzwerk zugreifen.

- Shared Key

  Ein geheimer, vordefinierter Schlüssel wird von allen Geräten verwendet, die auf das Wireless-Netzwerk zugreifen.

  Das Brother Wireless-Gerät verwendet den WEP-Schlüssel als vordefinierten Schlüssel.

- WPA-PSK/WPA2-PSK

  Aktiviert einen Wi-Fi Protected Access Pre-Shared Key (WPA-PSK/WPA2-PSK), einen gemeinsamen vordefinierten Schlüssel, der dem Brother Wireless-Gerät den Zugriff auf Access Points mit TKIP für WPA-PSK oder AES für WPA-PSK und WPA2-PSK (WPA-Personal) ermöglicht.

Verschlüsselungsmethoden

- Keine

  Die Daten werden nicht verschlüsselt.

- WEP

  Bei Verwendung von WEP (Wired Equivalent Privacy) werden die Daten mit einem Sicherheitsschlüssel gesendet und empfangen.

- TKIP

  TKIP (Temporal Key Integrity Protocol) ist eine Kombination aus einer Datenintegritätsprüfung (MIC) und einem Neuverschlüsselungsverfahren pro Datenpaket.

- AES

  AES (Advanced Encryption Standard) ist ein Wi-Fi®-autorisierter Standard für starke Verschlüsselung.

Netzwerkschlüssel

- Open System/Shared Key mit WEP

  Dieser Schlüssel ist ein 64-Bit- oder 128-Bit-Wert, der im ASCII- oder Hexadezimal-Format eingegeben werden muss.

  - 64 (40) Bit (ASCII):

    Verwendet 5 Textzeichen, z. B. „WSLAN“ (Groß-/Kleinschreibung beachten)

  - 64 (40) Bit (Hexadezimal):

    Verwendet 10-stellige Hexadezimal-Daten, z. B. „71f2234aba“

  - 128 (104) Bit (ASCII):

    Verwendet 13 Textzeichen, z. B. „Wirelesscomms“ (Groß-/Kleinschreibung beachten)

  - 128 (104) Bit (Hexadezimal):

    Verwendet 26 Zeichen im Hexadezimal-Datenformat, z. B. „71f2234ab56cd709e5412aa2ba“

- WPA-PSK/WPA2-PSK und TKIP oder AES

  Verwendet einen Pre-Shared-Schlüssel (PSK) von mindestens 8 und höchstens 63 Zeichen Länge.

Authentifizierungs- und Verschlüsselungsmethoden für Wireless-Netzwerke in Firmen und Unternehmen

Ein Wireless-Netzwerk für Firmen und Unternehmen ist ein großes Netzwerk. Wenn Ihr Gerät zum Beispiel in einer Firma oder einem Unternehmen an ein Wireless-Netzwerk mit IEEE 802.1x-Unterstützung angeschlossen ist und verschiedene Nutzer darauf zugreifen, handelt es sich um ein solches Netzwerk. Wenn Sie Ihr Gerät für ein Wireless-Netzwerk mit IEEE 802.1x-Unterstützung konfigurieren, können Sie die folgenden Authentifizierungs- und Verschlüsselungsmethoden verwenden.

Authentifizierungsmethoden

- LEAP

  Zu LEAP siehe *LEAP (für ein Wireless-Netzwerk)* auf Seite 9.

- EAP-FAST

  Zu EAP-FAST siehe *EAP-FAST* auf Seite 9.

- PEAP

  Zu PEAP siehe *PEAP* auf Seite 9.

- EAP-TTLS

  Zu EAP-TTLS siehe *EAP-TTLS* auf Seite 10.

- EAP-TLS

  Zu EAP-TLS siehe *EAP-TLS* auf Seite 10.

Verschlüsselungsmethoden

- TKIP

  Zu TKIP siehe *TKIP* auf Seite 12.
- AES

  Zu AES siehe *AES* auf Seite 12.
- CKIP

  Das original CKIP-Protokoll (Cisco Key Integrity Protocol) für LEAP von Cisco Systems Inc.

Benutzer-ID und Kennwort

Die folgenden Sicherheitsmethoden verwenden eine Benutzer-ID mit einer Länge von weniger als 64 Zeichen und ein Kennwort mit einer Länge von weniger als 32 Zeichen.

- LEAP
- EAP-FAST
- PEAP
- EAP-TTLS
- EAP-TLS (für Benutzer-ID)

4 Zusätzliche Netzwerkeinstellungen unter Windows®

Arten von zusätzlichen Einstellungen

Die folgenden Funktionen stehen zum Konfigurieren zusätzlicher Netzwerkeinstellungen zur Verfügung.

- Web Services (Windows Vista® und Windows® 7)
- Vertical Pairing (WLAN-Einrichtungsassistent) (Windows® 7)



Vergewissern Sie sich, dass sich der Hostcomputer und das Gerät entweder im gleichen Subnetzwerk befinden, oder dass der Router für die Datenübertragung zwischen den beiden Geräten richtig konfiguriert ist.

Installation für das Drucken im Netzwerk mit Web Services (Windows Vista® und Windows® 7)

Mit der Web Services-Funktion können Sie die im Netzwerk angeschlossenen Geräte überwachen. Sie ermöglichen auch die Druckertreiber-Installation über das Druckersymbol und das Anlegen eines WSD-Ports (Web Services-Port).



- Bevor Sie diese Einstellung vornehmen, müssen Sie die IP-Adresse Ihres Gerätes konfigurieren.
- Für Windows Server® 2008 müssen Sie Print Services installieren.
- Nur die Druckerunterstützung wird mit den Webservices installiert.

1. Legen Sie die Installations-CD-ROM ein.
2. Wählen Sie Ihr CD-ROM-Laufwerk/**install**/**driver**/**gdi**/**32** oder **64**.
3. Wählen Sie Ihre Sprache und doppelklicken Sie dann auf **DPInst.exe**.



Wenn das Fenster **Benutzerkontensteuerung** erscheint:

(Windows Vista®) Klicken Sie auf **Zulassen**.

(Windows® 7) Klicken Sie auf **Ja**.

4 (Windows Vista®)
Klicken Sie auf und wählen Sie dann **Netzwerk**.
(Windows® 7)
Klicken Sie auf , **Systemsteuerung**, **Netzwerk und Internet** und dann auf **Netzwerkcomputer und -geräte anzeigen**.

5 Der Web Services-Name des Gerätes wird mit dem Druckersymbol angezeigt. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie installieren möchten.



Hinweis

Der Web Services-Name des Brother-Gerätes besteht aus dem Modellnamen und der MAC-Adresse (Ethernet-Adresse) Ihres Gerätes (zum Beispiel Brother MFC-XXXX (Modellname) [XXXXXXXXXXXX] (MAC-Adresse / Ethernet-Adresse).

6 Klicken Sie im Pulldown-Menü auf **Installieren**.

Installation für das Drucken im Netzwerk im Infrastruktur-Modus, wenn das Vertical Pairing verwendet wird (Windows® 7)

Windows® Vertical Pairing ist eine Technologie, mit der sich Ihr Wireless-Gerät, das diese Funktion unterstützt, mit Ihrem Infrastruktur-Netzwerk über das PIN-Verfahren des Wi-Fi Protected Setups und der Web Services-Funktion verbinden kann. Außerdem ermöglicht diese Funktion die Druckertreiber-Installation über das Druckersymbol, das Sie im Bildschirm **Gerät hinzufügen** finden.

Sie können Ihr Gerät im Infrastruktur-Modus im Wireless-Netzwerk anschließen und dann mit dieser Funktion den Druckertreiber installieren. Gehen Sie dazu wie folgt vor:

Hinweis

- Wenn Sie die Web Services-Funktion Ihres Gerätes ausgeschaltet haben, müssen Sie sie wieder einschalten. Die Standardeinstellung für die Web Services Ihres Brother-Gerätes ist Ein. Sie können die Web Services-Einstellung über das Web Based Management (Webbrowser) oder mit BRAdmin Professional 3 ändern.
- Vergewissern Sie sich, dass Ihr WLAN Access Point/Router mit dem Kompatibilitätslogo für Windows® 7 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller Ihres Access Points/Router.
- Vergewissern Sie sich, dass Ihr Computer mit dem Kompatibilitätslogo für Windows® 7 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller Ihres Computers.
- Wenn Sie Ihr Wireless-Netzwerk mit Hilfe einer externen Wireless-Netzwerkkarte NIC (Network Interface Card) konfigurieren, vergewissern Sie sich, dass diese Netzwerkkarte mit dem Kompatibilitätslogo für Windows® 7 gekennzeichnet ist. Weitere Informationen erhalten Sie beim Hersteller der Wireless-Netzwerkkarte.
- Um einen Computer mit Windows® 7 als Registrar zu nutzen, muss er zuvor in Ihrem Netzwerk registriert werden. Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde.

1. Schalten Sie Ihr Gerät ein.
2. Stellen Sie am Gerät das Wi-Fi Protected Setup (PIN-Methode) ein.
   Informationen zur Einrichtung Ihres Gerätes mit dem PIN-Verfahren finden Sie unter „PIN-Verfahren des Wi-Fi Protected Setup verwenden“ im *Netzwerkhandbuch*.
3. Klicken Sie auf die Schaltfläche und dann auf **Geräte und Drucker**.
4. Wählen Sie **Gerät hinzufügen** im Dialogfeld **Geräte und Drucker**.
5. Wählen Sie Ihr Gerät und geben Sie die von Ihrem Gerät angezeigte PIN ein.
6. Wählen Sie das Infrastruktur-Netzwerk, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie dann auf **Weiter**.
7. Wenn Ihr Gerät im Dialogfeld **Geräte und Drucker** angezeigt wird, sind die Wireless-Konfiguration und die Druckertreiber-Installation erfolgreich abgeschlossen.

5 Sicherheitsbegriffe und -konzepte

Sicherheitsfunktionen

Sicherheitsbegriffe

- CA (Certificate Authority: Zertifizierungsstelle)

  Die Zertifizierungsstelle stellt digitale Zertifikate aus (vor allem X.509 Zertifikate) und gewährleistet die Bindung zwischen den Datenpaketen in einem Zertifikat.

- CSR (Certificate Signing Request: Zertifikatsignieranforderung)

  Mit der Zertifikatsignieranforderung wird bei der Zertifizierungsstelle die Ausstellung eines Zertifikates beantragt. Die Zertifikatsignieranforderung enthält Informationen zur Identifizierung des Antragstellers, einen vom Antragsteller generierten öffentlichen Schlüssel (den Public Key) sowie die digitale Signatur des Antragstellers.

- Zertifikat

  Ein Zertifikat verbindet einen Public Key mit einer bestimmten Identität. Mit dem Zertifikat kann überprüft bzw. bestätigt werden, dass ein Public Key zu einer bestimmten Person gehört. Sein Format ist im x.509-Standard festgelegt.

- CA-Zertifikat

  Ein CA-Zertifikat identifiziert die Zertifizierungsstelle (CA) und verfügt über einen eigenen privaten Schlüssel. Es verifiziert ein von der Zertifizierungsstelle ausgegebenes Zertifikat.

- Digitale Signatur

  Die digitale Signatur ist ein Wert, der mit einem kryptografischen Algorithmus berechnet und so an ein Datenobjekt angehängt wird, dass der Datenempfänger die Herkunft und Identität der Daten anhand der Signatur überprüfen kann.

- Public-Key-Kryptosystem

  Das Public-Key-Kryptosystem ist ein moderner Zweig der Kryptografie, bei dem die Algorithmen auf ein Schlüsselpaar (einen Public Key und einen Private Key) angewendet werden. Für die verschiedenen Rechenschritte des Algorithmus wird jeweils auf eine andere Komponente des Schlüsselpaares zugegriffen.

- Shared-Key-Kryptosystem

  Das Shared-Key-Kryptosystem ist ein Zweig der Kryptografie, bei dem der gleiche Schlüssel für zwei verschiedene Rechenschritte des Algorithmus verwendet wird, z. B. zur Verschlüsselung und Entschlüsselung.

Sicherheitsprotokolle

 **Hinweis**

Sie können die Protokolleinstellungen über das Web Based Management (Webbrowser) konfigurieren. Weitere Informationen finden Sie im *Netzwerkhandbuch*.

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

Diese Protokolle zur sicheren Kommunikation verschlüsseln die Daten, um vor Übergriffen zu schützen.

HTTPS

Das Internetprotokoll HTTP (Hyper Text Transfer Protocol) verwendet SSL.

IPPS

Das Internet-Druckprotokoll IPP Version 1.0 verwendet SSL.

SNMPv3

SNMPv3 (Simple Network Management Protocol, Version 3) stellt Benutzerauthentifizierung und Datenverschlüsselung für eine sichere Verwaltung von Netzwerkgeräten zur Verfügung.

Sicherheitsmethoden für das Senden und Empfangen von E-Mails



Sie können die Einstellungen für die Sicherheitsmethoden über das Web Based Management (Webbrowser) konfigurieren. Weitere Informationen finden Sie im *Netzwerkhandbuch*.

POP vor SMTP (PbS)

Dies ist eine Methode zur Benutzerauthentifizierung beim Senden von E-Mails über einen Client. Vor dem Senden einer E-Mail spricht der Client erst den POP3-Server an und erhält dadurch die Erlaubnis für den Zugriff auf den SMTP-Server.

SMTP-AUTH (SMTP-Authentifizierung)

SMTP-AUTH erweitert SMTP (das Internetprotokoll für den E-Mail-Versand) um eine Authentifizierungsmethode, die gewährleistet, dass die Identität des Senders bekannt ist.

APOP (Authenticated Post Office Protocol)

APOP erweitert POP3 (das Internet-Empfangsprotokoll) um eine Authentifizierungsmethode, die das Kennwort verschlüsselt, wenn der Client eine E-Mail empfängt.

SMTP über SSL

SMTP über SSL ermöglicht das Senden von verschlüsselten E-Mails unter Verwendung von SSL.

POP über SSL

POP über SSL ermöglicht das Empfangen von verschlüsselten E-Mails unter Verwendung von SSL.

A Anhang A

Mit Diensten arbeiten

Ein Dienst oder Service ist eine Ressource, auf die Computer, die über den Brother PrintServer drucken wollen, zugreifen können. Der Brother PrintServer stellt die folgenden vordefinierten Dienste bereit (mit dem Befehl SHOW SERVICE in der Fernkonsole des Brother PrintServers kann eine Liste der verfügbaren Dienste abgerufen werden). Geben Sie an der Eingabeaufforderung `HELP` ein, um eine Liste der unterstützten Befehle anzuzeigen.

Service (Beispiel)	Definition
BINARY_P1	TCP/IP-Binär
TEXT_P1	TCP/IP-Textservice (fügt am Ende jeder Zeile einen Wagenrücklauf ein)
PCL_P1	PCL-Service (schaltet PJL-kompatible Geräte in den PCL-Modus)
BRNxxxxxxxxxxxx	TCP/IP-Binär
BRNxxxxxxxxxxxx_AT	PostScript®-Service für Macintosh
POSTSCRIPT_P1	PostScript®-Service (schaltet PJL-kompatible Geräte in den PostScript®-Modus)

Dabei steht „xxxxxxxxxxxx“ für die MAC-Adresse (Ethernet-Adresse) Ihres Gerätes.

Weitere Verfahren zur Einrichtung der IP-Adresse (für fortgeschrittene Nutzer und Administratoren)

IP-Adresse mit DHCP konfigurieren

Das Dynamic Host Configuration Protocol (DHCP) ist eines von mehreren Protokollen zur automatischen Zuweisung von IP-Adressen. Wenn ein DHCP-Server in Ihr Netzwerk eingebunden ist, erhält der PrintServer seine IP-Adresse automatisch vom DHCP-Server und sein Name wird bei allen mit RFC 1001 und 1002 kompatiblen dynamischen Namensdiensten registriert.



Wenn Sie Ihren PrintServer nicht über DHCP, BOOTP oder RARP konfigurieren möchten, müssen Sie die Boot-Methode auf Statisch setzen, damit der PrintServer eine feste IP-Adresse erhält. Dies verhindert, dass der PrintServer versucht, eine IP-Adresse von einem dieser Systeme zu erhalten. Um die Boot-Methode zu ändern, verwenden Sie das Netzwerk-Menü Ihres Gerätes (nur Modelle mit Display), die BRAdmin-Anwendungen, das Remote Setup oder das Web Based Management (Webbrowser).

IP-Adresse mit RARP konfigurieren

Die IP-Adresse des Brother PrintServers kann auch mit der Funktion Reverse ARP (RARP) auf Ihrem Hostcomputer konfiguriert werden. Dazu wird die Datei `/etc/ethers` mit einem Eintrag wie dem Folgenden versehen (wenn diese Datei nicht vorhanden ist, können Sie diese erzeugen):

`00:80:77:31:01:07    BRN008077310107` (oder `BRW008077310107` für ein Wireless-Netzwerk)

Dabei ist der erste Eintrag die MAC-Adresse (Ethernet-Adresse) des PrintServers und der zweite Eintrag der Name des PrintServers (dies muss derselbe Name sein, der auch in der Datei `/etc/hosts` angegeben wurde).

Starten Sie den RARP-Dämon, falls er nicht bereits läuft. Der entsprechende Befehl dazu lautet je nach System `rarpd`, `rarpd -a`, `in.rarpd -a` oder ähnlich. Geben Sie `man rarpd` ein oder suchen Sie in Ihrer Systemdokumentation nach weiteren Informationen). Geben Sie bei einem Berkeley UNIX-basierten System den folgenden Befehl ein, um zu überprüfen, ob der RARP-Dämon läuft:

```
ps -ax | grep -v grep | grep rarpd
```

Bei AT&T UNIX-basierten Systemen geben Sie ein:

```
ps -ef | grep -v grep | grep rarpd
```

Der Brother PrintServer erhält die IP-Adresse vom RARP-Dämon, wenn das Gerät eingeschaltet wird.

IP-Adresse mit BOOTP konfigurieren

BOOTP ist eine Alternative zu RARP mit dem Vorteil, dass mit BOOTP auch die Konfiguration von Subnetzmaske und Gateway möglich ist. Um die IP-Adresse mit BOOTP zu konfigurieren, müssen Sie sich vergewissern, dass BOOTP auf Ihrem Hostcomputer installiert ist und ausgeführt wird. (Es sollte in der Datei `/etc/services` auf Ihrem Host als echter Service erscheinen. Geben Sie `man bootpd` ein oder suchen Sie in Ihrer Systemdokumentation nach weiteren Informationen.) BOOTP wird normalerweise über die Datei `/etc/inetd.conf` gestartet. Sie können es daher gegebenenfalls durch Entfernen des Zeichens „#“ vor dem BOOTP-Eintrag in dieser Datei aktivieren. So würde zum Beispiel ein typischer bootp-Eintrag in der Datei /etc/inetd.conf lauten:

```
#bootp dgram udp wait /usr/etc/bootpd bootpd -i
```

Bei manchen Systemen kann dieser Eintrag „bootps“ anstelle von „bootp“ lauten.



Hinweis

Um BOOTP zu aktivieren, löschen Sie einfach das Zeichen „#“ in einem Editor (ist das Zeichen „#“ nicht vorhanden, dann ist BOOTP bereits aktiviert). Bearbeiten Sie dann die BOOTP-Konfigurationsdatei (in der Regel `/etc/bootptab`) und tragen Sie den Namen, Netzwerktyp (1 für Ethernet), MAC-Adresse (Ethernet-Adresse) sowie IP-Adresse, Subnetzmaske und Gateway des PrintServers ein. Leider ist das Format dieser Einträge nicht standardisiert. Lesen Sie deshalb in Ihrer Systemdokumentation nach, wie diese Angaben einzutragen sind. (Bei vielen UNIX-Systemen gibt es dafür auch Beispielvorlagen in der bootptab-Datei, an denen Sie sich orientieren können.) Hier einige Beispiele für typische `/etc/bootptab`-Einträge: („BRN“ ist „BRW“ bei einem Wireless-Netzwerk.)

```
BRN310107 1  00:80:77:31:01:07 192.168.1.2
```

und:

```
BRN310107:ht=ethernet:ha=008077310107:\ip=192.168.1.2:
```

Manche Implementierungen der BOOTP-Hostsoftware reagieren nicht auf BOOTP-Anfragen, wenn kein Download-Dateiname in der Konfigurationsdatei enthalten ist. Erzeugen Sie in diesem Fall einfach eine Nulldatei auf dem Host und geben Sie den Namen dieser Datei und ihren Pfad in der Konfigurationsdatei an.

Wie bei RARP lädt der PrintServer beim Einschalten des Gerätes seine IP-Adresse vom BOOTP-Server.

IP-Adresse mit APIPA konfigurieren

Der Brother PrintServer unterstützt das APIPA-Protokoll (Automatic Private IP Addressing). Mit APIPA konfigurieren DHCP-Clients automatisch eine IP-Adresse und Subnetzmaske, wenn kein DHCP-Server verfügbar ist. Das Gerät wählt seine IP-Adresse aus dem Adressbereich von 169.254.1.0 bis 169.254.254.255. Die Subnetzmaske wird automatisch auf 255.255.0.0 und die Gateway-Adresse auf 0.0.0.0 eingestellt.

Standardmäßig ist das APIPA-Protokoll aktiviert. Sie können das APIPA-Protokoll über das Funktionstastenfeld des Gerätes (nur Modelle mit Display), mit BRAdmin Light oder dem Web Based Management (Webbrowser) deaktivieren.

IP-Adresse mit ARP konfigurieren

Falls Sie die BRAdmin-Anwendung nicht nutzen können und in Ihrem Netzwerk kein DHCP-Server vorhanden ist, können Sie auch den Befehl ARP verwenden. Der Befehl ARP ist auf Windows®-Systemen, auf denen das TCP/IP-Protokoll installiert ist, und auf UNIX-Systemen verfügbar. Geben Sie zum Verwenden von ARP den folgenden Befehl an der Eingabeaufforderung ein:

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

Dabei ist `ethernetaddress` die MAC-Adresse (Ethernet-Adresse) des PrintServers und `ipaddress` die IP-Adresse des PrintServers. Zum Beispiel:

- **Windows®-Systeme**

  Windows®-Systeme benötigen einen Bindestrich „-“ zwischen den einzelnen Zeichen der MAC-Adresse (Ethernet-Adresse).

  ```
  arp -s 192.168.1.2 00-80-77-31-01-07
  ```

  ```
  ping 192.168.1.2
  ```

- **UNIX-/Linux-Systeme**

  Auf UNIX- und Linux-Systemen muss in der Regel ein Doppelpunkt „:“ zwischen den einzelnen Zeichen der MAC-Adresse (Ethernet-Adresse) eingegeben werden.

  ```
  arp -s 192.168.1.2 00:80:77:31:01:07
  ```

  ```
  ping 192.168.1.2
  ```



Hinweis

Der Befehl arp -s kann nur innerhalb des gleichen Ethernet-Segment verwendet werden (d. h. es darf sich kein Router zwischen PrintServer und Betriebssystem befinden).

Ist ein Router vorhanden, können Sie BOOTP oder eine andere in diesem Kapitel beschriebene Methode verwenden, um die IP-Adresse festzulegen. Wenn Ihr Administrator das System für die Zuweisung von IP-Adressen über BOOTP, DHCP oder RARP konfiguriert hat, kann der Brother PrintServer seine IP-Adresse von jedem dieser Dienste beziehen. In diesem Fall müssen Sie den Befehl ARP nicht verwenden. Der ARP-Befehl funktioniert nur einmal. Aus Sicherheitsgründen können Sie den ARP-Befehl nicht verwenden, um die IP-Adresse des Brother PrintServers zu ändern, nachdem diese mit ARP erfolgreich konfiguriert wurde. Der PrintServer ignoriert dann jeden Versuch, dies zu tun. Wenn Sie die IP-Adresse ändern möchten, verwenden Sie dazu das Web Based Management (Webbrowser), TELNET (mit dem Befehl SET IP ADDRESS) oder setzen Sie den PrintServer auf die werkseitigen Einstellungen zurück (danach kann der ARP-Befehl wieder genutzt werden).

IIP-Adresse über die TELNET-Konsole konfigurieren

Sie können die IP-Adresse auch mit dem Befehl TELNET ändern.

TELNET ist eine effektive Methode zur Änderung der IP-Adresse des Gerätes. Voraussetzung dafür ist allerdings, dass im PrintServer bereits eine gültige IP-Adresse hinterlegt wurde.

Geben Sie an der Eingabeaufforderung `TELNET <command line>` ein, wobei `<command line>` für die IP-Adresse des PrintServers steht. Wenn die Verbindung hergestellt ist, drücken Sie die Eingabe- oder Enter-Taste, um „#“ anzuzeigen. Geben Sie das Kennwort „**access**“ ein. (Das Kennwort wird nicht auf dem Bildschirm angezeigt.)

Sie werden nun aufgefordert, einen Benutzernamen einzugeben. Geben Sie einen beliebigen Text ein.

Als Eingabeaufforderung wird nun `Local>` angezeigt. Geben Sie `SET IP ADDRESS ipaddress` ein, wobei `ipaddress` die IP-Adresse ist, die Sie dem PrintServer zuweisen möchten. (Fragen Sie Ihren Netzwerkadministrator, welche IP-Adresse verwendet werden soll.) Zum Beispiel:

```
Local> SET IP ADDRESS 192.168.1.3
```

Nun müssen Sie die Subnetzmaske einrichten. Geben Sie `SET IP SUBNET subnet mask` ein, wobei `subnet mask` die Subnetzmaske ist, die Sie dem PrintServer zuweisen möchten. (Fragen Sie Ihren Netzwerkadministrator, welche Subnetzmaske verwendet werden soll.) Zum Beispiel:

```
Local> SET IP SUBNET 255.255.255.0
```

Wenn Ihr Netzwerk nicht in Subnetze unterteilt ist, verwenden Sie eine der folgenden Standard-Subnetzmasken:

255.0.0.0 für Netzwerke der Klasse A

255.255.0.0 für Netzwerke der Klasse B

255.255.255.0 für Netzwerke der Klasse C

Die Zifferngruppe ganz links in der IP-Adresse beschreibt, um welche Art von Netzwerk es sich handelt. Der Wert dieser Zifferngruppe liegt im Bereich von 1 bis 127 für Netzwerke der Klasse A (z. B. 13.27.7.1), im Bereich von 128 bis 191 für Netzwerke der Klasse B (z. B. 128.10.1.30) und im Bereich von 192 bis 255 für Netzwerke der Klasse C (z. B. 192.168.1.4).

Wenn Sie ein Gateway (Router) verwenden, geben Sie dessen Adresse mit dem Befehl `SET IP ROUTER routeraddress` ein, wobei `routeraddress` die IP-Adresse des Gateways ist, das Sie dem PrintServer zuweisen möchten. Zum Beispiel:

```
Local> SET IP ROUTER 192.168.1.4
```

Geben Sie `SET IP METHOD STATIC` ein, um die IP-Adresse als statische Adresse zu konfigurieren.

Überprüfen Sie, ob Sie die IP-Daten richtig eingegeben haben. Geben Sie dazu `SHOW IP` ein.

Geben Sie `EXIT` oder Strg-D ein (halten Sie dazu zum Beispiel die Strg-Taste gedrückt und geben Sie „D“ ein), um die Arbeit mit der Remote Console (Fernkonsole) zu beenden.

B Stichwortverzeichnis

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

V

W

Z